



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**TESTING AND EVALUATION OF DYNASIG BIOMETRIC
PEN IN SUPPORT OF TACTICAL MILITARY AND LAW
ENFORCEMENT MISSIONS**

by

Kenton M. Odgers

March 2007

Thesis Advisor:
Co-Advisor:

James Ehlert
Pat Sankar

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE March 2007	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE Testing and Evaluation of DynaSig Biometric Pen in Support of Tactical Military and Law Enforcement Missions			5. FUNDING NUMBERS	
6. AUTHOR(S) Kenton M. Odgers				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE	
13. ABSTRACT <p>Existing access control methods depend on mechanisms that can either be copied or stolen. From passwords to identification cards, these forms of authentication and verification are unique only while they remain in possession of the owner. Signature-based authentication and verification however, while not implying the two-dimensional ink on paper, but rather the method with which a signature is made, is extremely unique and provides a method that cannot feasibly be duplicated or stolen. Thereby, this form of access control can be more beneficial to security issues and to the increasing awareness of identity management.</p> <p>The objective of this thesis is to test and evaluate the Bio-Pen® and its associated WebClient software leveraging the Cooperative Operations and Applied Science and Technology Studies (COASTS) field experimentation program as a vessel for equipment and idea testing, requirements and standards definition. This thesis will examine a new biometric technology in terms of access control as well as its associated software. The primary objective of this research is to develop a fundamental understanding of the doctrinal, technological, and operational considerations of how the Bio-Pen® can be utilized within the Department of Defense and Homeland Defense. To accomplish this objective, the Bio-Pen® and WebClient software will be tested and evaluated for use in the field to determine feasibility for future applications.</p>				
14. SUBJECT TERMS Signature Verification, Behavioral Biometrics, Dynamic Signature			15. NUMBER OF PAGES 92	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**TESTING AND EVALUATION OF DYNASIG BIOMETRIC PEN IN SUPPORT
OF TACTICAL MILITARY AND LAW ENFORCEMENT MISSIONS**

Kenton M. Odgers
Lieutenant, United States Navy
B.S., United States Naval Academy, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

**NAVAL POSTGRADUATE SCHOOL
March 2007**

Author: Kenton M. Odgers

Approved by: Mr. James Ehlert
Thesis Advisor

Dr. Pat Sankar
Co-Advisor

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Existing access control methods depend on mechanisms that can either be copied or stolen. From passwords to identification cards, these forms of authentication and verification are unique only while they remain in possession of the owner. Signature-based authentication and verification however, while not implying the two-dimensional ink on paper, but rather the method with which a signature is made, is extremely unique and provides a method that cannot feasibly be duplicated or stolen. Thereby, this form of access control can be more beneficial to security issues and to the increasing awareness of identity management.

The objective of this thesis is to test and evaluate the Bio-Pen® and its associated WebClient software leveraging the Cooperative Operations and Applied Science and Technology Studies (COASTS) field experimentation program as a vessel for equipment and idea testing, requirements and standards definition. This thesis will examine a new biometric technology in terms of access control as well as its associated software. The primary objective of this research is to develop a fundamental understanding of the doctrinal, technological, and operational considerations of how the Bio-Pen® can be utilized within the Department of Defense and Homeland Defense. To accomplish this objective, the Bio-Pen® and WebClient software will be tested and evaluated for use in the field to determine feasibility for future applications.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	OVERVIEW	1
B.	BACKGROUND	2
C.	RESEARCH QUESTIONS	3
D.	SCOPE OF THESIS	3
E.	RESEARCH METHODOLOGY	4
F.	THESIS ORGANIZATION	4
II.	SIGNATURE VERIFICATION TECHNOLOGY	7
A.	OVERVIEW	7
1.	Static Signature Recognition.....	7
2.	Dynamic Signature Recognition	8
B.	BEHAVIORAL BIOMETRICS	8
C.	SIGNATURE AS A BIOMETRIC	9
D.	SIGNATURE VERIFICATION PROCESS	10
E.	PERFORMANCE MEASURES.....	11
F.	COMPARISON OF VARIOUS BIOMETRICS.....	14
III.	DYNAMIC BIOMETRIC SYSTEMS, INC.	15
A.	OVERVIEW	15
B.	BIO-PEN®.....	16
C.	WEB CLIENT	16
D.	LOCKBOX	17
IV.	SIGNATURE-BASED VERIFICATION SYSTEM.....	19
A.	BIO-PEN® CONCEPT OVERVIEW	19
B.	BIO-PEN® SECURITY FEATURES	21
1.	Hardware	21
2.	Firmware	21
3.	Software	22
4.	Individual Variations.....	22
C.	APPLICATION FLOW – WEBCIENT.....	23
1.	Start.....	24
2.	WebClient Main Menu	24
3.	Registration	25
4.	Verification	31
5.	Administrator Features	33
D.	SUMMARY	38
V.	NPS SIGNATURE VERIFICATION TEST	39
A.	OVERVIEW	39
B.	EQUIPMENT LIST	39
1.	Hardware	39
2.	Software	40

C.	TEST ENVIRONMENT	41
D.	TEST PROTOCOL	42
E.	TEST ANALYSIS	42
1.	Basic Statistics	43
2.	Imposter Test Analysis	45
3.	Comparison Analysis	45
F.	TEST LIMITATIONS.....	47
G.	SUMMARY	48
VI.	CONCLUSION AND RECOMMENDATIONS.....	49
A.	SUMMARY DISCUSSION.....	49
B.	RECOMMENDATIONS FOR FURTHER RESEARCH	49
	APPENDIX A. NPS SIGNATURE VERIFICATION TEST SUMMARY	51
	APPENDIX B. INSTITUTIONAL REVIEW BOARD DOCUMENTS.....	67
	LIST OF REFERENCES	71
	INITIAL DISTRIBUTION LIST	73

LIST OF FIGURES

Figure 1.	Signature Verification Process [11].....	11
Figure 2.	Receiver Operation Characteristics (ROC) Curve [13]	13
Figure 3.	ROC Curve and DET Curve [4].....	13
Figure 4.	Bio-Pen® Layered Packages	17
Figure 5.	Bio-Pen® 3 [www.bio-pen.com], 25 February 2007.	21
Figure 6.	Detailed Web-Flow Diagram for the Bio-Pen® WebClient Application	23
Figure 7.	Bio-Pen® Dynamic Signature Verification System	24
Figure 8.	Bio-Pen® WebClient Main Menu	25
Figure 9.	Bio-Pen® Registration Start	26
Figure 10.	Bio-Pen® Registration Pending.....	27
Figure 11.	Bio-Pen® Registration Second Signature.....	28
Figure 12.	Bio-Pen® Registration with Variations too Large.....	29
Figure 13.	Bio-Pen® Registration Completed	30
Figure 14.	Bio-Pen® User Registration	30
Figure 15.	Bio-Pen® Verification Failed	31
Figure 16.	Bio-Pen® Verification Pass	32
Figure 17.	Bio-Pen® User Information.....	33
Figure 18.	Bio-Pen® Log Files	35
Figure 19.	Bio-Pen® Secure Zone	36
Figure 20.	Bio-Pen® Control Panel	36
Figure 21.	Bio-Pen® User List.....	37
Figure 22.	Bio-Pen® List	38
Figure 23.	Hardware used in NPS Signature Verification System.....	40
Figure 24.	Signature Enrollment Report	43
Figure 25.	Signature Verification Report	44
Figure 26.	Number of Verification Attempts per Signature Model (User) Report	44
Figure 27.	Number of Imposter Verification Attempts by Performance Measure.....	45

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Comparison of Popular Biometrics [12]	14
Table 2.	Bio-Pen® 3 Product Specifications [www.bio-pen.com], 25 February 2007.....	20
Table 3.	NPS COASTS Signature Verification Test Analysis Comparison.....	47

THIS PAGE INTENTIONALLY LEFT BLANK

LIST Of ABBREVIATIONS

BPL	Bio-Pen® LockBox
CAC	Common Access Card
COASTS	Cooperative Operations and Applied Science and Technology Studies
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
DBSI	Dynamic Biometric Systems, Inc.
DET	Detection Error Tradeoff
DoD	Department of Defense
EER	Equal Error Rate
FAR	False Accept Rate
FMR	False Match Rate
FNMR	False Non-Match Rate
FRR	False Reject Rate
GUI	Graphical User Interface
ID	Identification
MCU	Microcontroller
NPS	Naval Postgraduate School
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Proof of Concept
ROC	Receiver Operating Characteristics
SOP	Standard Operations Procedures
USB	Universal Serial Bus

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Jim Ehlert and Dr. Pat Sankar for introducing me to this subject, for their continuing help and advice, and for their knowledge and encouragement throughout the past nine months while I worked on this project. I thank all of the students, faculty, and contractors who were involved with the COASTS organization for their patience and signatures. I would especially like to thank Dr. Richard Kim of DynaSig Corporation for his insight, support, and meaningful answers to my many questions. Lastly, I would like to thank my wife, Courtney, for her understanding, help, and unwavering enthusiasm throughout this research.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OVERVIEW

Who is valid and who is invalid is a question posed by the 1997 Columbia Pictures movie, *Gattaca*. Through biometric testing, “Valid” and “In-valid” are managed in every aspect of the fictional society. However, how much truth exists in this film environment? In this depiction of the future, identity management is paramount to the success and safety of individuals. After an extensive process, an “In-valid” is able to assume the identity of one of the “Valid” by fooling the biometric devices controlling the society. The truth of the film surfaces in the weaknesses of the biometric verification devices as the false identity of the “In-valid” is accepted. Though the film was released in 1997, it depicts the already-present need for Identity Management with an ever-increasing need for better biometric technology.

This master thesis documents the findings of the initial testing and evaluation of the Bio-Pen® and its associated Webclient software leveraging the Cooperative Operations and Applied Science and Technology Studies (COASTS) field experimentation program as a vessel for equipment and idea testing, requirements and standards definition.

Currently, the rapidly growing importance of Identity Management exists in both military and commercial settings. Passwords, identification (ID) cards, and signature pads provide identity authentication and verification. These technologies, however, suffer from inherent weaknesses associated with the primary authentication factor that each employs. Within many organizations, controlled spaces are protected by as little as a 4-digit keypad entry code. While most U.S. military bases are double-checking all Department of Defense (DoD) ID cards with a quick bar code scan, it is ultimately the photo ID that allows access. A personal identification number (PIN) protects a Common Access Card (CAC) card and the information stored within it. Almost everything that can be accessed over the internet (email, bank accounts, etc.) requires a password. Electronic signature pads, similar to those found in department stores, only provide a visual check against a signature.

These forms of authentication and access control work quite well and do provide a form of security in various situations. However, the innate weakness inherent to all of them is that they can be stolen, copied, or forged. Passwords can be written down somewhere and stolen, while ID cards and signatures on paper alone can be forged or copied. Therefore, these various methods of security and protection are only accurate while they are known or in the possession of each specific owner or user. An urgent need exists for a means to accurately verify the identity of individuals who require access to controlled spaces and for specific user authentication. The Bio-Pen® responds to this shortfall by using a different factor of authentication- something a user can do.

A person's signature is used almost daily for verification in a multitude of instances. From signing the back of checks at a bank, to signing the electronic pads at department stores, to even signing countless forms and papers in everyday life, a signature is one of the most widely accepted forms of verification. DynaSig, headed by Dr. Richard Kim, created the Bio-Pen® as a method of authentication and verification utilizing a person's signature as a behavioral biometric. Through development of a dynamic signature based system that uses the unique biomechanics of an individual's signature, the Bio-Pen® is complimentary with other biometric technologies that serve to enhance war-fighter capability.

When used in conjunction with other biometric systems and security procedures, signature-based verification and authentication can become a primary tool in positively identifying individuals and in controlling access to secure areas. The primary objective of this research is to develop a fundamental understanding of the doctrinal, technological, and operational aspects of the Bio-Pen® and how it can best be utilized within the DoD and Homeland Defense.

B. BACKGROUND

This thesis is being conducted as part of the COASTS 2007 international field experimentation project which encompasses students and faculty from Naval Postgraduate School (NPS), supported by the Office of Naval Research Reservists and numerous commercial partners. As reflected by the increasing number of requests to NPS from the DoD and friendly nations, there is an immediate requirement for low-cost,

state-of-the-art, C4ISR equipment that is rapidly deployable and scaleable. A central goal of the COASTS field experimentation program is to demonstrate that NPS, in conjunction with friendly nation organizations, can utilize commercial off the shelf (COTS) capabilities into a larger system of systems to potentially satisfy technical and tactical mission requirements.

C. RESEARCH QUESTIONS

In researching the Bio-Pen® and the alternate biometric and access control methods a number of questions arose. This thesis specifically addresses the following queries:

- Can a signature-based biometric be implemented as a low-cost, highly accurate method for authentication and verification?
- Determine the Receiver Operating Characteristics (ROC) curve and specifically the optimal equal error rate of false accept and false reject rates for signature-based biometrics?
- Identify military and law enforcement missions / requirements for which this technology is best suited for?
- Identify the strengths and weakness of the Bio-Pen® in terms of tactical multi-national mission requirements?
- Discuss the plans, policy, and doctrinal considerations to best utilize the Bio-Pen®?
- What potential drawbacks and dangers are there in alternate biometrics?
- Discuss how the Bio-Pen® can enhance security environments, specifically with respect to access control?
- Identify the costs associated with implementing signature-authentication technology?
- Discuss the mission benefits stemming from implementation of this technology?
- How Bio-Pen® can be used as an additional biometric to augment the existing biometrics already in use (fingerprint, face and iris)?

D. SCOPE OF THESIS

This thesis will be beneficial in ascertaining the usefulness of alternative access control methods, namely the Bio-Pen®. It will promote a better understanding of the capabilities and limitations of existing access control and biometrics, and determine an

improved form of access control as well as the associated implementation strategy. A more effective and secure method of access control allows for greater security and authentication of users. This thesis serves to enhance the existing public key infrastructure (PKI) program with new ideas and technology and furthermore improve the value and effectiveness of access control methods for US Navy missions and operations.

E. RESEARCH METHODOLOGY

The methodology that was used to research this thesis consisted of the following:

1. Development of metrics and test plan - This phase included the necessary academic review of existing material on access control and the Bio-Pen® System. Additionally the research focused on desirable attributes (requirements development) from the end-user's perspective. Measures of Performance and Measures of Effectiveness (MOP/MOE) were created. These MOP/MOE were used to develop an effective test and evaluation plan and provided a group of parameters for the initial formulation of the simulation model.
2. Base-lining and experimentation - Once a testing and evaluation plan was created, base-lining was conducted to determine the false rejection rates. The data collected was in accordance with the MOP/MOE. Each test incorporated a variety of situations as well as taking into account the modularity and ease with which it was incorporated into the testing. Data was collected from source experts, users, and actual tests performed in various environments which include, but are not limited to, Fort Hunter Liggett, Camp Roberts, and the Naval Postgraduate School.
3. Analysis of results and conclusions - The final phase consisted of analyzing the results of the Bio-Pen®. The results were compared to the base-lined system. They were also compared to the MOP/MOE's determined in Phase 1. By comparing the results from the alternatives to the base-line and MOP/MOE's, it was possible to determine the effectiveness and feasibility of deploying the technology in real-world military environments.

F. THESIS ORGANIZATION

This thesis consists of several chapters that can be grouped into four main parts:

Chapter II embodies the “why.” It describes the background behind signature verification as well as the need for this technology versus other biometrics. Cost-

effective and secure methods of access control and biometrics will assist the US Military and the Department of Homeland Defense in current and future missions and operations. This chapter will also explore the field of behavioral biometrics.

Chapters III and IV embody the “what.” They describe the concepts as well as the emergent technology available. Chapter III discusses DynaSig Corporation, and how their product suite can be employed to provide a more secure operational environment. Chapter IV investigates the concept of using the Bio-Pen® technology, illustrating its potential instantiations as well as its various strengths and weaknesses.

Chapter V embodies the “how.” The system requirements for a signature-based biometric, as well as use of the Bio-Pen® as an access control method are described. An example of how a system would work in a tactical field setting is provided from experimentation and results gathered.

Chapter VI concludes the thesis with directions for continued research on this topic and summarizes the concepts and results presented in this body of work.

THIS PAGE INTENTIONALLY LEFT BLANK

II. SIGNATURE VERIFICATION TECHNOLOGY

A. OVERVIEW

“The pen is mightier than the sword” is an adage coined by the playwright Edward Bulwer-Lytton in 1839. Indeed, the power of a pen has been recognized through the centuries, long before this famous quote was originated. Similarly, signature verification, also known as signature authentication, is not a new technology.¹ Dating back to the 1970s, considerable research in this field has occurred in academia and the commercial sectors [1]. With the exponential growth in computational processing power and in sensor technology, signature verification has now become a viable form of biometric technology.

Signature verification is, at the very least, the process used to recognize the hand-written signature of an individual. Signature verification is of particular importance as it is the only widely accepted method for endorsing financial transactions [2]. In the categorization of signature recognition, two separate methods are used to perform signature verification, static signature recognition and dynamic signature recognition. This thesis focuses on the latter of the two technologies.

1. Static Signature Recognition

Static signature recognition, sometimes referred to as off-line verification, processes signature verifications through the analysis of the shape of a signature. It is concerned with the signature made by a normal pen that is digitized through an optical device. A static signature can be analyzed through measurements of the following features [3]:

- Number of component strokes
- Ratio of long to short strokes

¹ The terms verification and authentication are often used interchangeably, however, there exists a slight difference between the terms. Verification refers to the process of comparing a signature sample against a signature template in the system associated with a claimed identity. Authentication refers to a similar process that uses verification to allow certain privileges to the identity being verified. Authentication also means that the verified entity can be linked to the claimed identity (verified by other independent means collected during a prior registration process such as photo ID or fingerprint etc.)

- Curvature of measurements
- Segment lengths

These features allow the static approach, through difficulty of limited data, to process signature verification. Performance of a static system is much weaker and expectedly lower than that of a dynamic system due to a static system's inability to take advantage of the dynamic handwriting process. [1] [4]

2. Dynamic Signature Recognition

Dynamic signature recognition, also known as on-line verification, captures a signature as it is being written in real-time. A variety of input devices from digitizing tablets to stand-alone pens acquire the signature in real-time and capture the following features [5]:

- Timing measurements
- Stroke order
- Pen velocity profiles
- Pen acceleration profiles
- Pen up/pen down patterns

Through the combination of the aforementioned features, a digital signature template is created that offers more reliable identity protection than a static system could provide. Most of the features captured in a dynamic system do not leave their shape in the final image making it more difficult to forge, as well as making the shape ultimately less meaningful [1]. The DynaSig (Dynamic Signature) Bio-Pen® system utilizes the on-line verification method which will be the only method discussed throughout the remainder of this thesis. For additional information regarding the topic of signature verification refer to references [1], [2], [3], [5] and [10].

B. BEHAVIORAL BIOMETRICS

Biometrics support identity management through one of two main categories [6]:

- Physiological Biometrics: Direct measurement of a part of the human body (e.g., fingerprint, hand geometry, face, iris)

- Behavioral Biometrics: Data and measurements derived from an action performed by the user. This is an indirect measure of some characteristics of the human body. Dynamic Signature Verification falls under this category.

Behavioral biometrics maximizes the potential of natural models for user recognition. Systems that capture and store fingerprints or iris patterns can cause many users to be hesitant to accept the solution. Also, many of the devices required by these systems can be very intrusive in the scanning process [7]. Conversely behavioral devices are more accepted, especially signature verification, as it is the only widely adopted method for endorsing financial transactions [2].

There are advantages in behavioral biometrics that cannot be employed in physiological biometrics. While physical features remain relatively constant over time, behavioral characteristics can change over the short and long term due to user control, health, physiological state and aging. To increase security, users are required to change a password after a designated amount of time. Similarly, users can alter their behavior over time to increase the security of their biometric. Also, in certain circumstances, users can hide their true identity by creating false negatives. Consciously changing the behavior being measured can aid individuals who do not wish to cooperate in adverse situations.

C. SIGNATURE AS A BIOMETRIC

The USA National Institute of Standards and Technology defines biometric systems as “automated methods of recognizing a person based on physiological or behavioral characteristics” [8]. At the same time, the need for secure, fast and non-intrusive identification of people as a primary goal for homeland security has spawned from recent global terrorism. A commonly used biometric, the signature, has long been accepted in government, legal, and commercial transactions as the sole method of verification and authentication. With regards to biometrics, a unique, identifying characteristic exists in the manner in which a person signs his or her name [9].

A signature is a personal behavior developed over time by a user and is an action that becomes very consistent. While variations do exist from signature to signature, the pen accelerations, pen up and pen down movements, and the time element to sign are habitually consistent [10]. Compared to other behavioral biometric method such as voice

authentication, dynamic signature verification is language independent. Specific software is not required for signature verification to span several different languages. Since the measurements of a dynamic signature are focused around the neuro-muscular movements of the pen, a signature can be in any language or take any form of consistent pen movements. Utilizing the signature as a biometric presents several other advantages [14]:

- The signature is perhaps the most natural and generally established of all the ways in which a user seeks to confirm identity.
- The use of signature verification will minimize the disruption to accepted practices with respect to transactions where personal identity has to be authenticated.
- Measurement of signature characteristics is non-invasive (compared to iris scanning) and has no negative or undesirable health connotations [3].
- It is highly resistant to impostor attempts. Replicating the dynamic information of a signature from the digitized template is impossible in determining how a person signed their signature. Concomitantly, the visual observation of a person signing does not display certain variables such as pressure.
- The user can change his or her signature. While most biometrics cannot be changed (fingerprint, iris, etc.), the ability to change a signature like a password circumvents this drawback [6].

Unfortunately, there is no perfect biometric method, as even signature verification presents its own set of drawbacks:

- Signature variability due to lack of habit. This can be overcome through proper training and practice.
- Influenced by physical and emotional conditions. Users under varying degrees of stress, or users with a broken arm have varying signatures [6].

D. SIGNATURE VERIFICATION PROCESS

The basic structure for a signature verification system is shown in Figure 1. A signature verification system has two distinct phases, the first is the enrollment phase and the second is the verification phase. In the enrollment, or registration phase, the signature is first processed to extract features conveying dynamic information, and then a signature model is created based on the collected data. This data is then stored in a database for later reference during the verification phase. In the verification phase, the signature is again processed to extract features conveying dynamic information; however, this time

instead of creating a signature model, the signature verification system implements a likelihood ratio test to distinguish between two hypotheses to determine if the signature originates from the claimed signer or from an imposter. Features extracted from the signature are compared to a model representing the claimed signer (obtained from a previous enrollment) and a percentage, or ratio is determined based on the amount of variations between the two models. This percentage, or ratio, is then compared to a set threshold to decide whether to accept or reject the signature. This matching process must take into account the variations in the dynamic features and can utilize one of three categories of methods [2] [6]:

- Template Matching – The signature and template are expressed as feature vectors and compared using a distance measure between them.
- Stochastic – A statistical model is created through the extraction of features in the registration signatures. During verification, the similarity of the signature and reference to the model are established.
- Neural Networks – Require large amounts of genuine and forgery signatures, which are not always available.

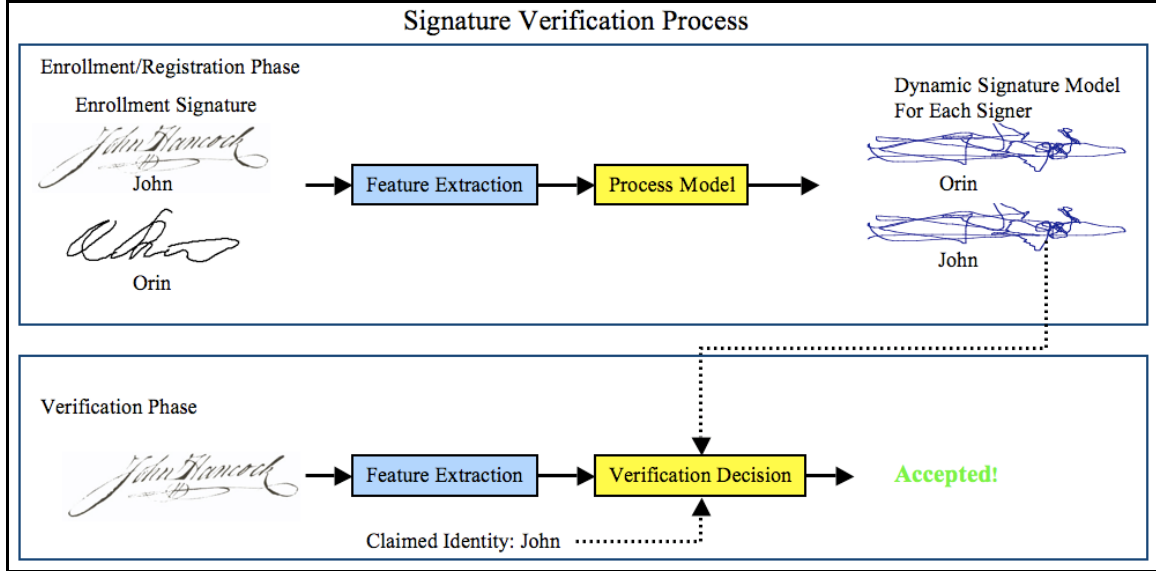


Figure 1. Signature Verification Process [11]

E. PERFORMANCE MEASURES

Performance of a signature verification system is based on the measure between two types of errors found in biometric systems. The two types of errors that can occur in

biometric systems are False Match Rate (FMR) and False Non-Match Rate (FNMR), more commonly referred to as False Accept Rate (FAR) and False Reject Rate (FRR) [10].

- False Match, or False Accept, is the false acceptance of an invalid user, such as in the case of an imposter breaking into a system (also known as a Type-I error).
- False Non-Match, or False Reject, is the false rejection of a valid user, such as in the case of rejecting a true signer (also known as a Type-II error) [4].

The tradeoff between FAR and FRR is present in every biometric system. However, the tradeoff varies from system to system. For example, if one system's threshold is programmed for greater security, the probability of false rejections would increase (FRR rises) while the probability that an imposter breaks into the system is reduced (FAR decreases). Conversely, if another system's threshold is positioned to allow greater user convenience, the odds of receiving a false rejection (FRR) decreases, and the chance that an imposter can break into the system (FAR) increases. The differences that occur at various threshold levels can be depicted in the form of a receiver operating characteristic (ROC) curve. Illustrating system performance at all the operating points (thresholds), a ROC curve is a plot of FAR against FRR for these various operating points for a given application. An example of an ROC curve is shown in Figure 2, which shows the optimal area for any application, where both types of errors are equal. This point is also referred to as the Equal Error Rate (EER) [4][12].

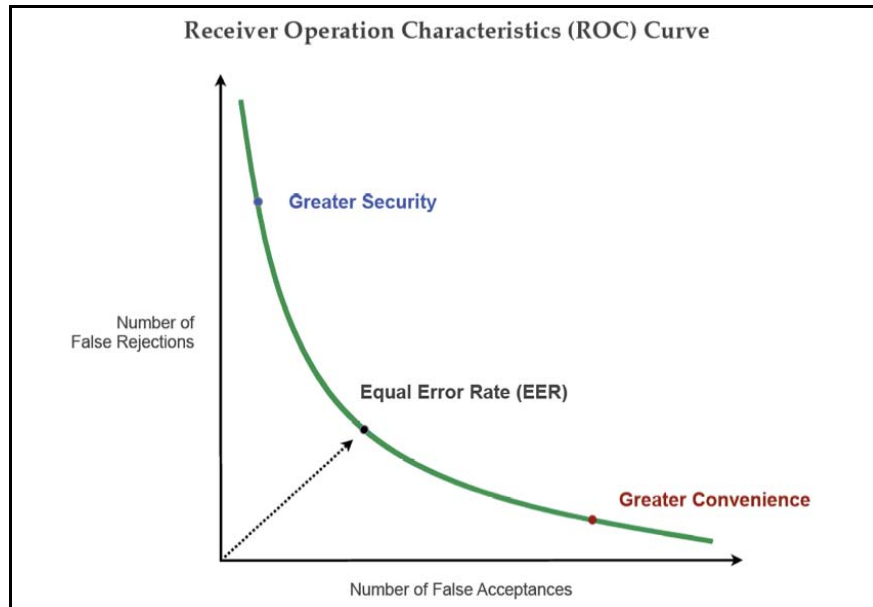


Figure 2. Receiver Operation Characteristics (ROC) Curve [13]

More recently, a variant of an ROC curve, called the detection error tradeoff (DET) curve, has been employed to provide a clearer visualization of competitive systems. The DET curve plots the same tradeoff as the ROC curve, but uses a normal deviate scale [4]. This reduces the bunching effect of curves in the lower left corner when performance is high and produces a more linear curve. The advantage of a DET curve is that system comparisons are easier to perform, especially those with multiple data sets. Figure 3 shows the comparison of a system using both the ROC curve and the DET curve.

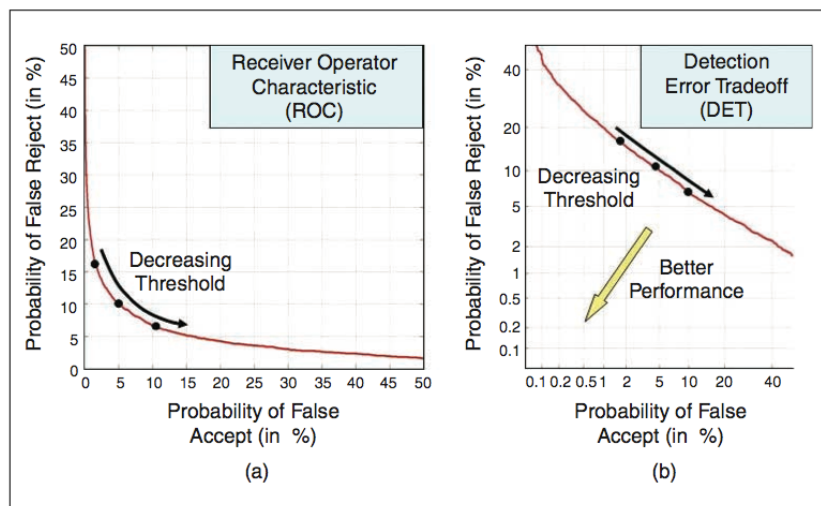


Figure 3. ROC Curve and DET Curve [4]

F. COMPARISON OF VARIOUS BIOMETRICS

How does signature verification compare to other forms of biometrics? A number of biometric characteristics used in various applications exist to answer that question. Each biometric has its own strengths and weaknesses, while the choice of which biometric to employ depends on the application. No single biometric is expected to meet the requirements of all the possible applications. The combination of several verification methods, also known as multimodal, improves the overall performance without relying on only one technology [4]. Depending upon the perceived user profiles, the need to interface with other systems or databases, environmental conditions, cost, and the properties of the biometric characteristic all determine which biometric is best suited for an application [12]. Table 1 presents a comparison of the leading forms of biometric systems.

Comparison of Biometrics							
Characteristics	Fingerprint	Hand	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error Incidence	Dryness, dirt, age	Hand injury, age	Glasses	Poor lighting	Lighting, age, glasses, hair	Changing Signatures	Noise, colds, channel variables
Accuracy	High	High	Very high	Very high	High	High	High
User Acceptance	Medium	Medium	Medium	Medium	Medium	Very high	High
Required Security Level	High	Medium	High	Very high	Medium	Medium	Medium
Long Term Stability	High	Medium	High	High	Medium	Medium	Medium

Table 1. Comparison of Popular Biometrics [12]

III. DYNAMIC BIOMETRIC SYSTEMS, INC.

A. OVERVIEW

Headquartered in Phoenix, Arizona, DynaSig, Inc. produces a verification system based on signature or handwriting biometrics. DynaSig publicly trades under their parent corporation, Dynamic Biometric Systems, Inc. (DBSI). Incorporated on June 17, 2003, DynaSig was founded by current CEO, Richard Kim, Ph.D. He holds undergraduate, graduate, and doctorate degrees in electrical engineering. While working with the U.S. Navy, Army, Air Force, and NASA, Dr. Kim developed an extensive background in sensor technology and signal processing [11]. This experience and education gave Dr. Kim the intellectual inspiration to develop a biometric identification system. He currently holds seven issued patents and has an additional three patents pending. Dr. Kim's crowning achievement has been the conceptual invention of the Bio-Pen® System, an innovative biometric identification system. Primary clients of DynaSig who have invested in this system are banking and other security-related industries [15] [16].

The Bio-Pen® System consists of the Bio-Pen®, a signature capturing mechanism, and the WebClient and LockBox software, which completes the registration and authentication aspects of the system. Through the acquisition of a previous IBM patent, the Bio-Pen® System can offer the advantages of the highest security identification and most private verification systems in the personal biometric authentication market today [17]. Unlike conventional biometric systems, the Bio-Pen® system utilizes the dynamic characteristics of a person's unique behavior that cannot be easily imitated. At the same time, the system protects the privacy of the user since no personal information can be recreated using the stored data. Dynamic biometric systems are very flexible, easy to implement, and have a high acceptance rate by the users. [11]

Provided in this chapter is a general overview of DynaSig's Bio-Pen®, WebClient and LockBox software. The below information was gathered from datasheets that are readily accessible from DynaSig's website at <http://www.dynasig.com/>.

B. BIO-PEN®

The foundational product for the DynaSig Corporation is the dynamic signature-based biometric pen called the Bio-Pen®. This pen so closely resembles the look and feel of a typical ink pen that a user is unable to tell the difference. The Bio-Pen® has the following advantages when compared to other biometric identification options [14]:

- It is multi-factor authentication and uses both behavioral and physical characteristics as determining biometric identifiers.
- It is a natural model, well accepted, and easy to implement in an organization and requires no learning curve or "social" engineering.
- It cannot be intercepted or copied the way fingerprints or other physical biometrics can.
- Unlike most voice biometrics, the Bio-Pen is language independent of the user.

The Bio-Pen®, which will be discussed at length in the next chapter, aims to solve identity theft and access control issues by providing a more secure and private biometric solution.

C. WEB CLIENT

With Internet businesses becoming mainstream, their survival depends on providing customers with a secure and reliable place to do business. The Bio-Pen® WebClient software provides this security with a registration and verification interface. [17]

The Bio-Pen® WebClient can be used with the Internet, through remote access, or with server based applications. With a multitude of applications, the WebClient can be integrated into a variety of security mechanisms [18]:

- Authenticated document release system with real signature.
- Access control, verification, and logs.
- Visa and Passport verification.
- Funds transfer and withdrawal within the banking system.
- Credit Card processing for secure Internet purchases. [11]

The WebClient played an important role in the testing phase for this thesis and details of the registration and verification process will be outlined in a subsequent chapter.

D. LOCKBOX

The Bio-Pen® Lockbox (BPL) utilizes the same method of verification as the WebClient, while adding greater functionality for advanced document control. The BPL allows the creation of documents that assure the identity of both the sender and receiver. When used with any secure email attachment application, the Lockbox created will only be accessible by the sender and receiver but will also carry the ability to hold multiple documents created from a variety of programs. These possibilities can be word processing documents, blueprints, or even audio and video files [18].

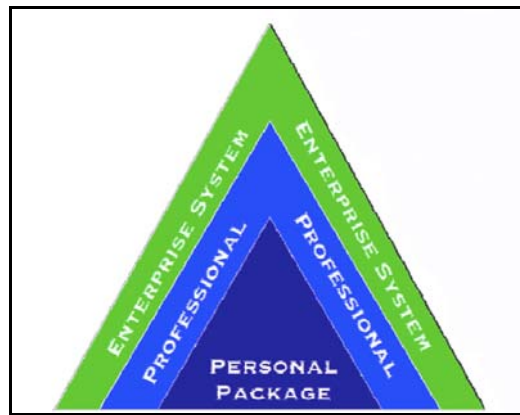


Figure 4. Bio-Pen® Layered Packages

The DynaSig Bio-Pen® system is currently available in several packages [19]:

- **The Bio-Pen® Personal Package** represents the most basic application of the Bio-Pen system, by including a Bio-Pen® with USB interface and the WebClient and LockBox software. Compatible with any e-mail system, the Lockbox software verifies the sender and the receiver's identity. This security feature allows for the transmission of multiple documents, which can be anything from a word processing document to a video file [20].
- **The Professional Edition** extends the functions of the Bio-Pen Personal Package by allowing secure electronic document transmission among multiple users [21].

- **The Enterprise System** permits an entire organization, through their internal network, to utilize the basic functions of the Professional and Personal Packages. Additional capabilities are complete audit trails of documents, viewers, and signers [22].

IV. SIGNATURE-BASED VERIFICATION SYSTEM

A. BIO-PEN® CONCEPT OVERVIEW

A signature-based verification system, in its most common form, is comprised of an electronic signature pad that is used to capture information about a signature. Through measurements of an associated input device, the electronic pad is able to create a digital signature. However, with advancements in sensor technology, the necessity for an entire pad has become inconsequential. The only device needed for a signature-verification system today is a writing utensil. Through the incorporation of sensors into the tool used most often to perform a signature, DynaSig is able to generate a secure digital signature [23].

As previously discussed, biometric authentication is determined by at least one of three factors unique to an individual. The three most common factors for authentication methodologies are:

- Something the user *knows* (e.g., password, PIN)
- Something the user *has* (e.g., ID card, smart card)
- Something the user *is* (e.g., biometric characteristic, such as a fingerprint or iris scan)

The purpose of the DynaSig Bio-Pen® System is to take advantage of a unique characteristic that utilizes all three of these authentication factors as well the incorporation of a fourth factor [14]:

- Something the user *can do* (e.g., signature using the Bio-Pen®)

Through the proprietary intellectual properties held by DynaSig, the Bio-Pen® is able to determine a person's signature in three dimensions, not just the two-dimensional ink on paper. The physical movement of the pen in the X, Y, and Z direction is recorded by the custom hardware and verified by the Bio-Pen® System WebClient.

There are many DoD and Homeland Defense applications envisioned for the use and integration of this system:

- Secure access to controlled spaces – Rather than use a keypad, a person would be required to sign to gain access.
- Document approval/authorization – Not only would there be a digital signature to accompany the document, but it would also verify the signer.
- Gate access – Instead of a visual check of an ID card, persons requesting entrance would use their signature.
- Verification by boarding party – After registering in the originating port, Navy and Coast Guard boarding parties could verify the identity of vessel crews.
- Email digital signature – Replacing the PKI certificate, a Bio-Pen® signature doesn't require an approving authority and isn't stored in a way that can be compromised.

This chapter will explore the specifics of the Bio-Pen® and its associated software, WebClient, to include the security features as well as the application flow of the web-based verification system. Table 1 lists the detailed product specifications for the latest iteration, the Bio-Pen® 3 USB.

Product Specifications - Bio-Pen® 3 USB	
Capture Method:	Pen movement sensor system not requiring a dedicated writing surface
Pen Size (L x D):	134 x 13mm (5.3 x 0.5 inches)
Pen Weight:	25 grams (0.9 ounces)
LED Functions:	Orange - Power on Green Blinking - Ready to sign Green On - Pen tip in contact with writing surface
Ink Life (pen refill):	> 7,000 signatures
Z-Pressure:	256 levels
Interface to Host:	Standard USB 1.0/1.1/2.0 interface, mini B 4-pin female connector
Power:	Powered from USB host
Data Transfer Rate	4,096 bits/second
Operating Conditions:	10 C to 40 C; maximum 90% R.H., non-condensing
Storage Conditions:	0 C to 60 C; maximum 90% R.H., non-condensing
Matching Algorithm:	DynaSig Corporation proprietary
Enrollment Time:	Typically 7 seconds (1 second automatic delay per signature)
Template Size:	Typically 500 bytes
Matching Speed:	Less than 1 second

Table 2. Bio-Pen® 3 Product Specifications [www.bio-pen.com], 25 February 2007.

B. BIO-PEN® SECURITY FEATURES

While not providing true encryption, the Bio-Pen® System does possess several security features in its hardware, firmware, software and individual variations imposed by the user. Through these multiple layers of security, it is very difficult for an imposter to decode the system behavior.

1. Hardware

The Bio-Pen® is made up of non-standard motion sensors that are embedded within the metal casing. The custom sensors have the ability to capture motion in the X, Y, and Z planes, as well as pressure that is exerted on the pen tip. The pen tip itself is interchangeable with the option of an ink tip or plastic stylus tip that is inserted into the pen by unscrewing the bottom portion. Figure 5 shows how the Bio-Pen® appears as an ordinary pen to the casual observer. [24]

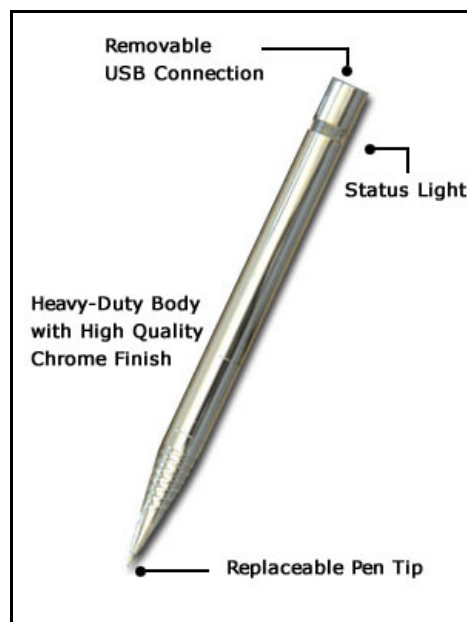


Figure 5. Bio-Pen® 3 [www.bio-pen.com], 25 February 2007.

2. Firmware

Within the hardware of the pen resides the custom microcontroller (MCU). The MCU is a single integrated circuit with the central processing unit (CPU), input/output interfaces (USB), memory, and analog-to-digital converters. This firmware has been

specially developed in order to pre-process the data it receives from the sensors embedded in the pen. Each Bio-Pen® has a unique serial number that not only identifies the pen itself, but also provides a unique ID that the firmware uses to attach to the authentication algorithm. Also, the firmware creates a second distinctive feature by receiving a unique code from the host software. This unique code, or time-stamp, is generated real-time, which means that it changes the next time the pen is used making it only valid for the one instance of the signature. [24]

3. Software

The data that is captured from the Bio-Pen® carries with it the two unique attributes generated by the firmware. The authentication algorithm constructs the digital signature from these two unique attributes and the input from the signature itself. This input is then compared to the template located in the database for the specified User ID. Through custom programming of the authentication algorithm, the system is able to verify the similarities between the input and the template. This algorithm takes into account a replay of the same input as a failure due to the two firmware-generated unique attributes that make up the digital signature. Similarly, the software can detect if the data has been corrupted or tampered with during the verification. [24]

4. Individual Variations

As discussed earlier, behavioral biometrics, and more specifically signature biometrics, rely less on physical characteristics such as a fingerprint or iris scan, and more on the unique neuro-muscular memory of a person's writing behavior. Due to this focus, variations arise in an individual's signature each time he or she writes it. More importantly, in the case of the Bio-Pen®, an individual may know what his or her signature is, but not so much how to actually perform it. The difficulty arises in trying to describe the process that a person uses to write his or her signature. With this main advantage, the unique signature of an individual cannot be copied, stolen, or even given to anyone else. With each verification attempt, the various parameters that comprise the

digital signature are continually changed, from the time-stamp to even personal variations in the signature performed. This allows the output data to be different each attempt, only to be decoded by the system authentication algorithm. [24]

C. APPLICATION FLOW – WEBCLIENT

The following discussion provides a description of Bio-Pen® System WebClient Web-Flow including the actual screen prompts. Figure 6 is a diagram of the described process. The WebClient was the primary application used during the NPS Cooperative Operations and Applied Science and Technology (COASTS) Signature Verification Tests.

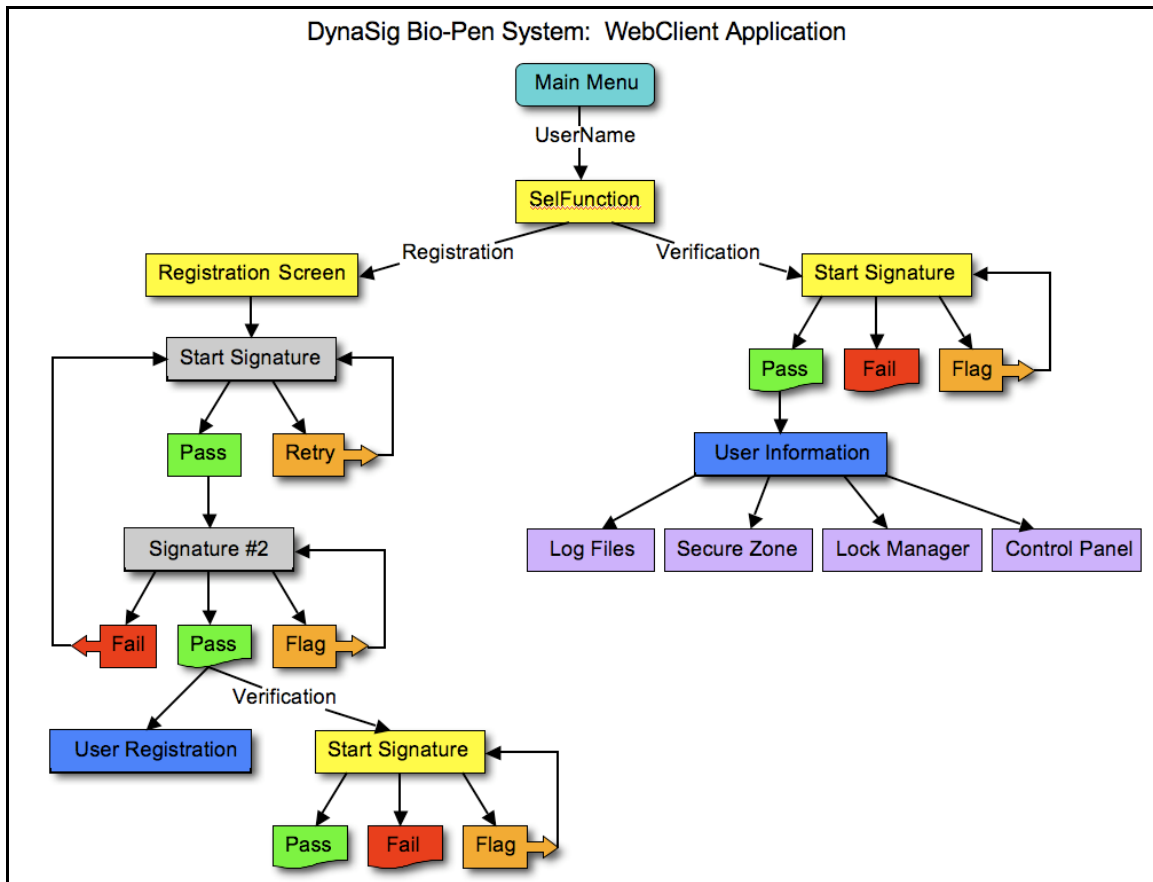


Figure 6. Detailed Web-Flow Diagram for the Bio-Pen® WebClient Application

1. Start

When initially starting the system, a splash screen of the Bio-Pen® Dynamic Biometric logo greets the user. After a moment, the user is taken to the Bio-Pen® Web Access page at <http://www.bio-pen.com/BioAttendance/>. Once the page loads, it performs an immediate check to see if a Bio-Pen® is connected and displays a status message. Figure 7 shows the simple setup required to use the Bio-Pen®.

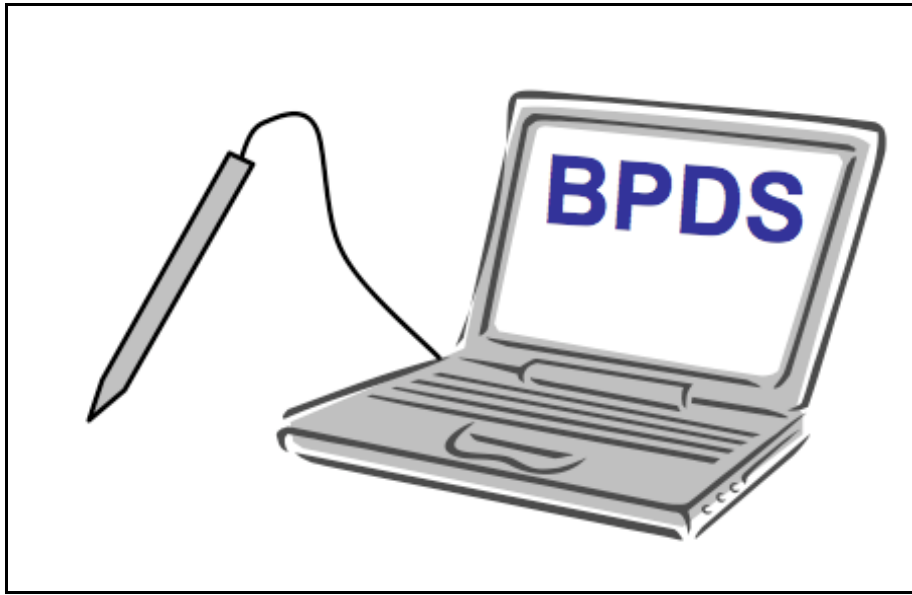


Figure 7. Bio-Pen® Dynamic Signature Verification System

2. WebClient Main Menu

Once a Bio-Pen® is connected, the Pen ID is displayed in the main menu. At this point, a user can choose to create a new user account, or verify an existing account. Also, should the user change pens, he or she can check the Pen ID of the current pen. The LED light on the Bio-Pen® will be red in color to show that it is connected to the system. Figure 8 shows the WebClient main menu.



© Copyright 2003 - 2006 DynaSig Corporation All Right Reserved.

Figure 8. Bio-Pen® WebClient Main Menu

3. Registration

With a Bio-Pen® connected to a system, users can create a user name following the greater than 4-character constraint, as long as the user name has not been taken. To begin, the user enters a valid User ID into the main menu and clicks the “Register” button. This takes the user to the registration screen. Following the onscreen prompts, the user is asked to click the “Start” button and then perform his or her signature. Figure 9 shows the Bio-Pen® registration screen.



Figure 9. Bio-Pen® Registration Start

Once completed, the system will provide immediate signature quality feedback as a function of four variables.

- Length – How long (time) was the signature
- Character – How many distinct pen movements are in the signature
- Pressure – How much pressure was exerted by the user
- Movement – How much movement is detected by the pen body

The maximum score possible is 100 points. DynaSig recommends at least two stars in each category to increase the security level of the signature. Figure 10 shows the Bio-Pen® registration pending screen.



© Copyright 2003 - 2007 DynaSig Corporation All Right Reserved.

Figure 10. Bio-Pen® Registration Pending

The system will then request the user to sign once more to complete the registration. The system will display the message “Registration pending: click ‘START’ to sign.” The user will click the “Start” button and then perform his or her signature just as he or she did the first time. Each time the user signs on the registration screen, signature quality will be immediately displayed. Figure 11 shows the Bio-Pen® registration “sign one more time” screen.

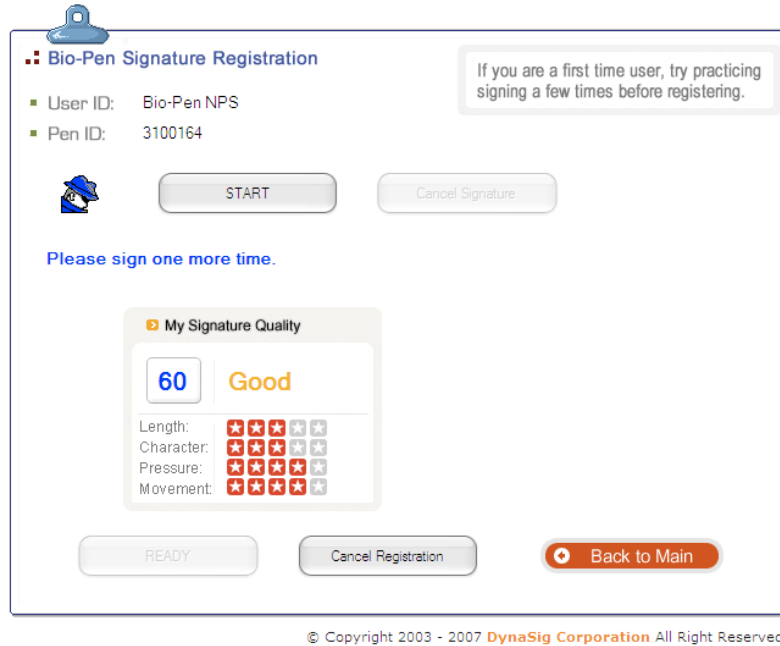


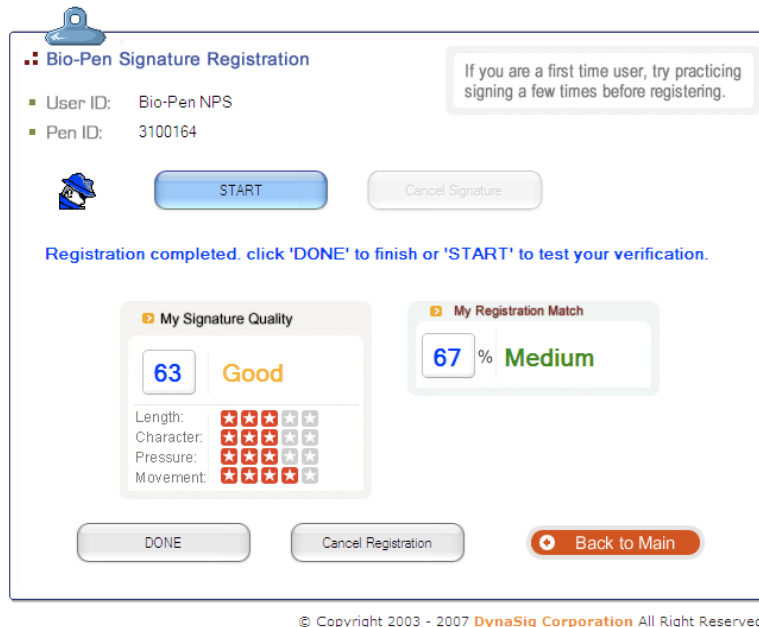
Figure 11. Bio-Pen® Registration Second Signature

If there are too many variations between the first and second signature registrations, the system will ask the user to sign again. In this case, the system will display the message, “Variations too large: sign again or ‘Cancel Registration’ to start over. This is a result of the custom algorithm that calculates the dissimilarity between the two signatures. The user can repeat his signature, or start the registration process over again. Figure 12 shows the Bio-Pen® failed registration screen.



Figure 12. Bio-Pen® Registration with Variations too Large


If the second registration signature is accepted by the system, the registration will be complete. At this point, a registration match percentage will be displayed with feedback along with the message, “Registration completed. Click ‘DONE’ to finish or ‘START’ to test your verification.” The registration percentage is based on the amount of variation between the registration signatures, or how closely they match. The more variation detected by the system, the lower the percentage assigned. DynaSig recommends any registration with a value less than 60% in the “My Registration Match” window should cancel the registration and try again. Users have the option of testing their registration signature by performing an instant verification by clicking the “Start” button. This option can be performed as many times as the users desires. Or, the user can click “Done” to complete the registration process. Figure 13 shows the Bio-Pen® registration completed screen.



Bio-Pen Signature Registration

If you are a first time user, try practicing signing a few times before registering.
































User ID: Bio-Pen NPS
Pen ID: 3100164



Registration completed. click 'DONE' to finish or 'START' to test your verification.

My Signature Quality

63 Good

Length:                               

4. Verification

Ensuring the Bio-Pen® is connected to the system, user verification takes place from the WebClient main screen. After entering a User ID, the person requesting verification will click the “Start” button and then perform his signature. The Bio-Pen® LED light will turn green and blink indicating that it is ready to use. If the signature does not match the registration for the specified User ID, the system will return the following message, “Verification Failed. Please try again.” Currently, there is no upper limit on the number of times a signature entered can fail verification before the User ID is locked out for a period of time. Figure 15 shows the Bio-Pen® failed verification screen.

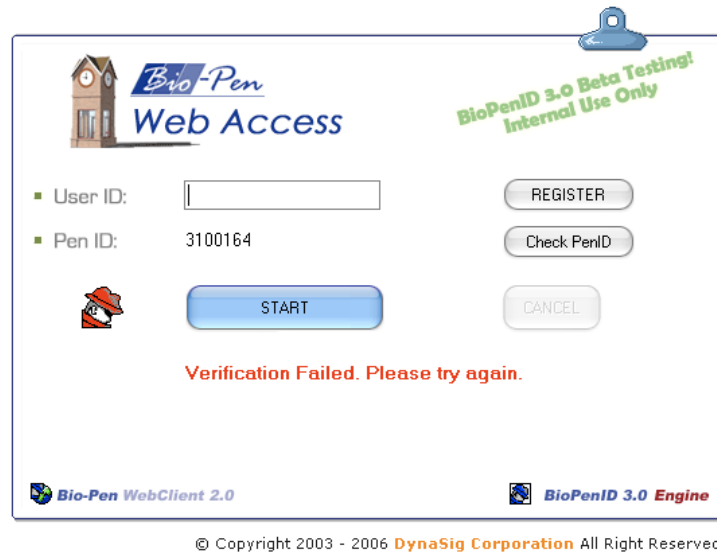






Figure 15. Bio-Pen® Verification Failed

If the signature matches within the parameters assigned by the custom algorithms limits, the system reports the following message “PASS ... Going to Secure Zone ...” and navigates to the user information page. Figure 16 shows the Bio-Pen® verification accepted screen.




Figure 16. Bio-Pen® Verification Pass

The following page is the main user page once the signature has been verified. Several functions can be performed from this page. Personal information can be updated as well as other tasks that are detailed in the administrative features section. Figure 17 shows the Bio-Pen® user information screen.

User ID: Kent Odgers
 Pen ID: 3100164 (Enterprise)
 Group ID: NPS
 Authority: ADMIN

[My Account](#)
[LOGOUT](#)



■ MY ACCOUNT

Status	Edit
Registered	Edit

■ BIO-PEN INFORMATION

Owner ID	Status	Register Date	Mode	Edit
kent odgers	Activate		Enterprise	Edit

■ PERSONAL INFORMATION

First Name:
 Last Name:
 Company:
 E-mail:
 Phone:
 Address:
 City:
 State/Province:
 Zip:
 Country:

Registered date: 1/16/2007 6:59:12 PM

© Copyright 2003 - 2007 DynaSig Corp. All Right Reserved.

DynaSig Corporation

Figure 17. Bio-Pen® User Information

5. Administrator Features

There are many administrative features available in the Bio-Pen® WebClient. Currently, however, there are some features that are for demonstration purposes only. The navigation for the administrative features is located at the top of the page to the left of the user information. These features are listed below:


- Log Files – Logs user activity for all pens associated with the Group ID
- Secure Zone – Demonstration for other applications
- Control – User and Pen control panel
- Lock Manager – Interface to download “Buddy Locks” for use with the LockBox application²


² This feature is not discussed further in this thesis due to the lack of testing with this function. It is recommended that further testing utilizing the LockBox utility be performed to adequately assess its function.


The Log Files page contains a detailed log of all pen activity for the specific Group ID. The log has the following columns:

- User ID – Registration User ID
- Company – Group ID
- Auth – Authorization level (e.g., Admin, User)
- Pen SN – Bio-Pen® serial number
- Activity – Action performed that triggers the log file (e.g., Verification, Registration Pending)
- Log Date – Date and Time of log entry
- User IP – IP address where activity originated
- Result – Activity result (e.g., Pass, Denied, Flag, Register)
- Detail – Contains specific data of the activity. The entry for the detail column is read as follows:
 - Example: PASS/1/60/67/64/60/67/80
 - PASS – Result
 - 1 – Number code for result
 - 60 – Match percentage
 - 67 – Average signature quality score
 - 64 – Length score
 - 60 – Character score
 - 67 – Pressure score
 - 80 – Movement score
- Impos – Imposter setting for testing (True = Imposter attempt)

Figure 18 shows the Bio-Pen® administrator log files screen.

Log Files


Secure Zone

Control


User ID: **Kent Odgers**
Pen SN: **3100164**
Group ID: **NPS**
Authority: **ADMIN**

My Account

LOGOUT

Bio-Pen
Dynamic Biometric ID

LOG FILES

User ID 

Search

Show All

Total Logs: 84

(NPS)

User ID	Company	Auth	Pen SN	Activity	Log Date	User IP	Result	Detail	Impos
Kent Odgers	NPS	Admin	3100164	Verification	2/22/2007 5:09:52 PM	70.134.75.6	Pass	PASS/1/60/67/64/60/67/80	False
Kent Odgers	NPS	Admin	3100164	Verification	2/22/2007 5:09:44 PM	70.134.75.6	Denied	DENW-55/57/73/65/70/80/77	False
Kent Odgers	NPS	Admin	3100164	Verification	2/22/2007 5:09:35 PM	70.134.75.6	Denied	DENW-55/51/63/56/50/68/80	False
Kent Odgers	NPS	Admin	3100164	Verification	2/22/2007 5:09:26 PM	70.134.75.6	Denied	DENW-55/41/61/47/50/67/82	False
Kent Odgers	NPS	Admin	3100164	Verification	2/22/2007 5:09:18 PM	70.134.75.6	Denied	DENW-55/50/55/54/50/56/63	False
Kent Odgers	NPS	Admin	3100164	Verification	2/22/2007 5:09:10 PM	70.134.75.6	Denied	DENW-55/59/58/56/60/47/70	False
Kent Odgers	NPS	Admin	3100164	Verification	2/22/2007 5:09:01 PM	70.134.75.6	Denied	DENW-55/31/59/44/60/53/80	False
Bio-Pen NPS	NPS	User	3100164	Verification	2/22/2007 5:07:42 PM	70.134.75.6	Register	RGCP/11/67/63/60/60/59/74	False
Bio-Pen NPS	NPS	User	3100164	Register Pending	2/22/2007 5:07:17 PM	70.134.75.6	Flag	RGIC/-55/43/66/63/60/59/82	False
Bio-Pen NPS	NPS	User	3100164	Register Pending	2/22/2007 5:06:48 PM	70.134.75.6	Register	RGOM/-60/34/60/50/60/65/68	False
thesis	NPS	User	3100164	Verification	2/19/2007 10:59:12 PM	205.155.65.236	Pass	PASS/1/69/48/12/30/62/91	False
thesis	NPS	User	3100164	Verification	2/19/2007 10:59:08 PM	205.155.65.236	Flag	FLAG/4/65/43/11/30/46/87	False
thesis	NPS	User	3100164	Verification	2/19/2007 10:59:04 PM	205.155.65.236	Flag	FLAG/4/66/40/11/40/48/61	False
thesis	NPS	User	3100164	Verification	2/19/2007 10:58:45 PM	205.155.65.236	Pass	PASS/1/76/35/11/30/36/65	False
thesis	NPS	User	3100164	Verification	2/19/2007 10:58:40 PM	205.155.65.236	Pass	PASS/1/71/32/11/20/53/46	False
thesis	NPS	User	3100164	Verification	2/19/2007 10:58:35 PM	205.155.65.236	Pass	PASS/12/85/34/12/30/50/45	False
thesis	NPS	User	3100164	Register Pending	2/19/2007 10:58:29 PM	205.155.65.236	Register	RGCP/10/80/35/15/30/48/48	False
thesis	NPS	User	3100164	Register Pending	2/19/2007 10:58:23 PM	205.155.65.236	Register	RGPD/14/0/31/18/30/36/43	False
Kent Odgers	NPS	Admin	3100164	Verification	2/19/2007 10:42:58 PM	70.134.114.175	Pass	PASS/1/68/63/67/70/38/79	False
Kent Odgers	NPS	Admin	3100164	Verification	2/19/2007 10:42:50 PM	70.134.114.175	Denied	DENW-55/55/59/68/50/50/69	False
1 2 3 4 5									

Figure 18. Bio-Pen® Log Files

The next administrative feature is the Secure Zone. This feature is for demonstration purposes only to illustrate the use of the Bio-Pen® in various online industries. A unique digital signature creates more security when using any of the mentioned examples:

- Internet Banking
- Shopping
- Signature Verification
- Document Approval

- Secure Message
- eMortgage

Figure 19 shows the Bio-Pen® secure zone screen.



Figure 19. Bio-Pen® Secure Zone

The last feature of the administrative set to be discussed is the control panel. This is where basic administrative controls can be exerted over users and Bio-Pens that are part of the Group ID. Figure 20 shows the Bio-Pen® control panel screen.

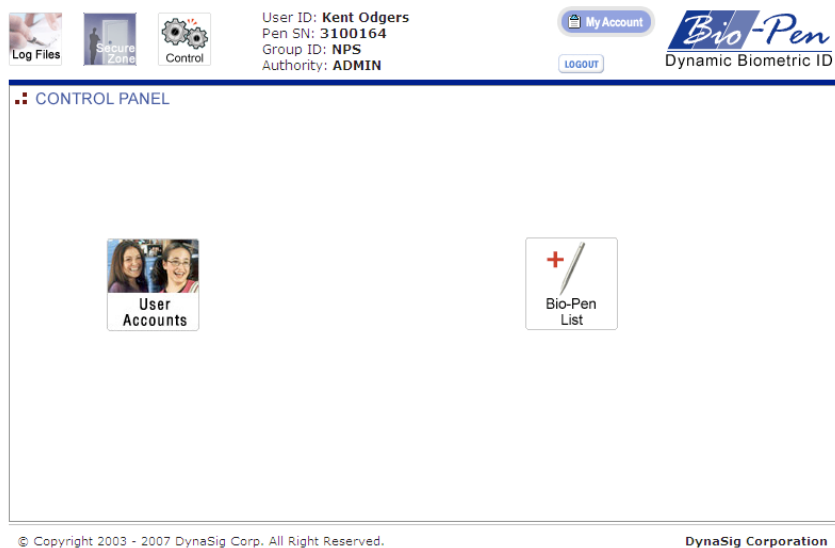


Figure 20. Bio-Pen® Control Panel

The user accounts page lists the total number of users that belong to the Group ID. Users can be created, deleted, or modified (forcing a new registration) from this page. There is also a search function in the case that the number of users extends past the first page, or if there is a specific query requested. Figure 21 shows the Bio-Pen® user list screen.

USER LIST

Total Number of Users: 92 (NPS)

User ID	Status	Date Modified	Edit	Delete
Billy Bob	Registered	1/18/2007 8:24:58 PM	Edit	X
billybob	Registered	1/19/2007 2:59:32 PM	Edit	X
Bio-Pen NPS	Registered	2/22/2007 5:05:41 PM	Edit	X
corkyo	Registered	1/21/2007 12:31:19 PM	Edit	X
drwells	Registered	2/12/2007 5:43:01 PM	Edit	X
ericwhy	Registered	2/14/2007 2:11:22 PM	Edit	X
joe navy	Registered	1/19/2007 1:21:32 PM	Edit	X
kento	Registered	1/17/2007 9:54:54 AM	Edit	X
navalpostgrad	Registered	2/12/2007 5:02:30 PM	Edit	X
pat test1	Registered	1/17/2007 2:22:53 PM	Edit	X
pat test2	Registered	1/17/2007 2:23:27 PM	Edit	X
redteam1	Registered	1/20/2007 10:17:38 AM	Edit	X
redteam2	Registered	1/20/2007 10:23:48 AM	Edit	X
redteam3	Registered	1/20/2007 10:29:47 AM	Edit	X
redteam4	Registered	1/20/2007 10:31:02 AM	Edit	X
testing	Register Pending	2/14/2007 2:11:20 PM	Edit	X
thesis	Registered	2/19/2007 10:45:46 PM	Edit	X
user10a	Registered	1/17/2007 4:08:13 PM	Edit	X
user10b	Registered	1/17/2007 4:12:19 PM	Edit	X
user10c	Registered	1/17/2007 4:15:43 PM	Edit	X

1 2 3 4 5

© Copyright 2003 - 2007 DynaSig Corp. All Right Reserved. DynaSig Corporation

Figure 21. Bio-Pen® User List

The Bio-Pen® list page displays the Bio-Pens that belong to the specific Group ID. Each pen can be assigned an Owner ID that gives that user the ability to not enter his User ID on the main page of the WebClient. Instead, the verification function uses the Bio-Pen® serial number that is assigned to only one specific user. Also, the Bio-Pen® details can be edited from this page much like the user list page. Figure 22 shows the Bio-Pen® list screen.





User ID: **Kent Odgers**
 Pen SN: **3100164**
 Group ID: **NPS**
 Authority: **ADMIN**

My Account

LOGOUT



■ BIO-PEN LIST

Pen SN

Search

Show All

Total Number of Pen: 6

Pen SN	Group ID	Release Date Modified	Owner ID	Date Modified	Status	Mode	Edit
3100164	NPS	4/3/2006 9:46:47 PM	kent odgers	1/16/2007 6:53:25 PM	Activate	Enterprise	Edit
3100163	NPS	4/3/2006 9:53:32 PM		1/16/2007 4:11:42 PM	Activate	Enterprise	Edit
3100161	NPS	4/3/2006 9:48:52 PM			Activate	Enterprise	Edit
3100159	NPS	3/14/2006 11:54:34 AM			Activate	Enterprise	Edit
3100156	NPS	3/14/2006 9:26:57 AM	ericwhy	2/14/2007 2:15:08 PM	Activate	Enterprise	Edit
3100153	NPS	3/14/2006 9:26:08 AM	Pat Sankar	2/1/2007 4:24:23 PM	Activate	Enterprise	Edit

Figure 22. Bio-Pen® List

D. SUMMARY

In this chapter, the Bio-Pen® System was discussed in detail regarding the security features of the Bio-Pen® and the application flow of the WebClient. The security features of the Bio-Pen® combined with the WebClient application provided the base for a signature-based verification system. The system features an easy enrollment and registration process, as well as a simple verification process. As evident by the security features, user information recreation is extremely difficult if not impossible thereby protecting the privacy of the user. There is a great amount of flexibility with the system, and can be used in multiple situations:

- Simple and easy local verification (e.g., point-of-sales applications)
- Remote verification (e.g., Internet applications)
- High security verification (e.g., access control and financial applications)

Through the use of the signature as a unique biometric, the Bio-Pen® System demonstrates the feasibility of using low-cost COTS technologies in order to create a signature-based verification system with high levels of security and ease of implementation into existing systems.

V. NPS SIGNATURE VERIFICATION TEST

A. OVERVIEW

The purpose of the NPS COASTS Signature Verification Test was to create an initial testing of the DynaSig Bio-Pen® System utilizing the performance measures of false reject rate (FRR) and false accept rate (FAR). This test was conducted using DynaSig's packaged dynamic biometric signature application, Bio-Pen® Enterprise System using their WebClient 2.1. All of the signatures collected during the testing were performed with one of the five NPS-purchased Bio-Pens, each with individual serial numbers. Powered by DynaSig's BioPenID 3.0 Engine, the Bio-Pen® Enterprise System uses sensor technology to capture the physical and behavioral characteristics of the "way" in which a person performs their signature in a true digital signature. Please refer to Appendix A for a detailed test log.

B. EQUIPMENT LIST

For this test, the following equipment (hardware and software) were used to test and to demonstrate this application.

1. Hardware

Based on the software requirements of DynaSig, a machine running Windows XP was needed in order to conduct this test. Due to the lack of abundant hardware, as well as the author's own personal preference, a personal laptop was used in conjunction with a virtual machine running Windows XP. For testing purposes, the following hardware was used, see Figure 23.

- Apple MacBook Pro 17" Intel Core 2 Duo Processor (2.33 GHz), 2 GB 667 MHz DDR2 SDRAM, 160GB Hard Drive, Apple AirPort Extreme Wireless (802.11 a/b/g, 54 Mbps) and integrated Bluetooth.
- DynaSig Bio-Pen® USB, custom hardware, sensors, and firmware.

The laptop computer was chosen for its processing power, memory capability, mobility, battery life, and familiarity. Compared to similar models by other

manufacturers, the Apple MacBook exhibits extraordinary battery life that allows for extended testing in the field without plugging in to an external power supply. DynaSig requires Microsoft's Windows 2000, NT, or XP. In order to use Windows NT 4.0, Service Pack 6a is required. Also, the Microsoft Data Access Components (MDAC) 2.6 update and .NET Framework version 1.1 or newer are required [25].

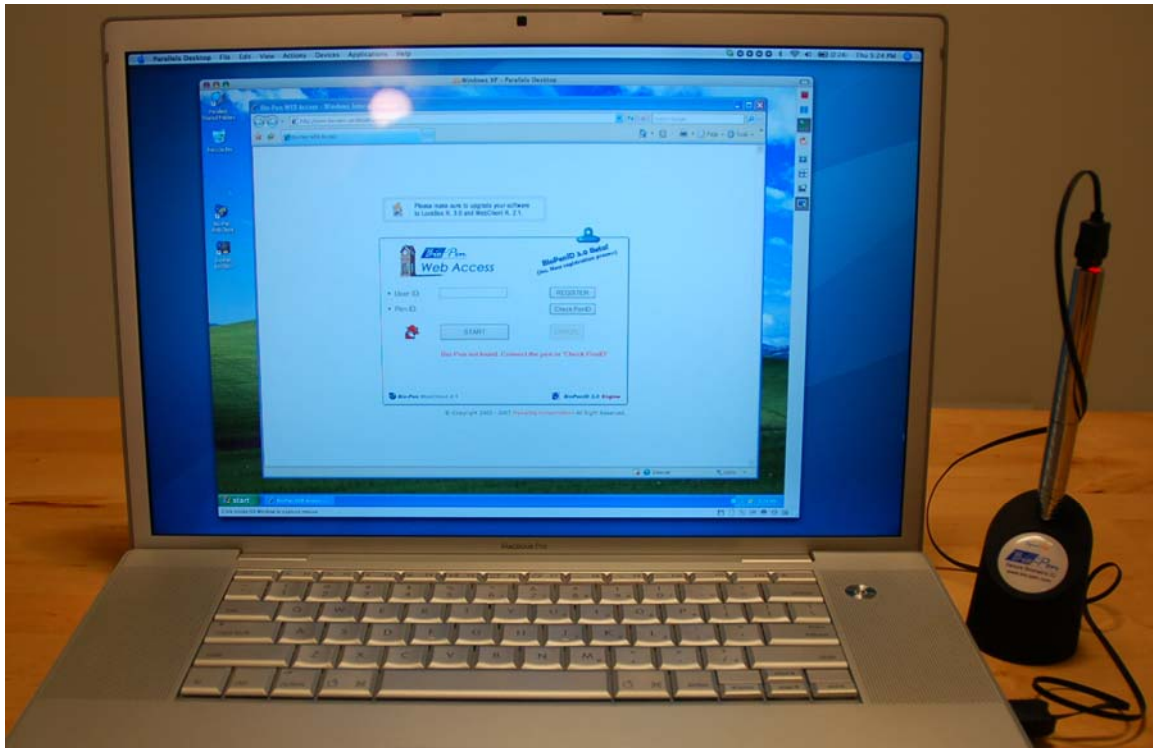


Figure 23. Hardware used in NPS Signature Verification System

2. Software

Listed below are the software applications used to conduct this test:

- Apple OSX 10.4
- Parallels Desktop for Mac
- Microsoft's Windows XP Professional
- Microsoft's Internet Explorer
- Bio-Pen® WebClient 2.1

For this test, the Bio-Pen® system was only tested using Microsoft Windows XP, but is capable of operating with Windows 2000 and NT. In order to use the Bio-Pen®

WebClient, Internet Explorer 7 was required. The Bio-Pen® hardware connects directly to the computer through the USB port. However, it is noted that the Bio-Pen® USB drivers are only available for the Windows based operating systems. There is also a solution for users of Windows XP Service Pack 2 available from the DynaSig website, http://www.bio-pen.com/Page/BioPen_Guide_XPSP2.htm. The current configuration of the Bio-Pen® hardware limits the USB connectivity due to the drivers that negate the use of other operating systems. Parallels Desktop for Mac is virtualization software for Intel-based Mac computers that allows users to run a Windows operating system concurrently within the Apple OS. Parallels was chosen for its compatibility with the MacBook Pro as well as the Bio-Pen® System. This software can be purchased and downloaded from Parallels' website at <http://www.parallels.com/en/download/desktop/>. Parallels Desktop for Mac is fully functional virtual machine software with USB support that enables Windows-based drivers to be used in Apple hardware.

C. TEST ENVIRONMENT

The NPS COASTS Signature Verification Test was conducted alongside various technologies comprising the Test 2 for the COASTS 2007 field experimentation program. The Bio-Pen® System was setup near the main network operations centers which was located at Fort Hunter Liggett, California. All signatures collected were performed with the Bio-Pen® hardware connected via USB cable to the Apple MacBook Pro running Windows XP Professional. Throughout the testing, separate environmental variables were noticed but not included in the analysis. These variables could be used to determine the accuracy of the system under less than ideal conditions. The variables that were observed focus on the effects of the temperature during the testing: cold weather and gloves.

- Cold weather was determined to be in the range of observed temperatures from 16°F to 40°F. While this temperature range had little effect on the hardware used during testing, it did have an adverse affect on the signature testing. During the COASTS 2007 Signature Verification Test, signatures were collected at various times during the day at varying temperatures.
- As a direct result of the cold weather, users that wore an insulating surface to cover their hands also had an adverse affect on the signature testing. The majority of users were not wearing gloves during the registration and verification process.

D. TEST PROTOCOL

The test protocol for the signature verification test consisted of four steps. In step one, invitations were verbally issued to all participants of the COASTS 2007 Test 2 requesting volunteers to participate in this research. The invitation included a general overview of the Bio-Pen® System, as well as printed applicable consent forms. As part of the NPS/DOD regulations for the use of human subjects, the COASTS research team obtained permission from the NPS Institutional Review Board prior to conducting any testing. For additional information on the Institutional Review Board documents refer to Appendix B of this thesis. In step two, on specified test dates (17-20 Jan 07), and in conjunction with the larger Test 2, participants were asked to sign their name to register and verify their signature biometric. Participants were given the opportunity to register during the testing hours on four successive days. In step three, participants were asked to verify their signature at random intervals post registration. During the registration process, participants were asked to register with the system using their most familiar, repeatable signature and assigned a unique identification number. At a minimum, two signatures were gathered and used to generate a unique model of the participant's signature. Participants were then given the opportunity to additionally register a generic phrase as well as a custom phrase of their choice. During the verification process, the participants provided their identification number and signature a minimum of one time. Finally, in step four, the results of the COASTS Signature Verification Test were compiled and used for analysis.

E. TEST ANALYSIS

The analysis of the COASTS Signature Verification Test was conducted in three phases. The first phase consisted of an analysis of the signature log (basic statistics) of the registration and verification test, resulting in a single data-point analysis. The second phase consisted of an analysis of the separate imposter test conducted alongside the normal verification data set, resulting in a second single data-point analysis. The third phase consisted of a comparison of the two single data-point analyses. [26]

1. Basic Statistics

Provided in Figures 24 through 27 are the summary of the basic statistics of the NPS Signature Verification Test.

Figure 24 presents the aggregate signature enrollment data, which consisted of 40 test subjects enrolled during the COASTS Test II, with a 26-user enrollment with a custom phrase and a 12-user enrollment with a given, generic phrase.

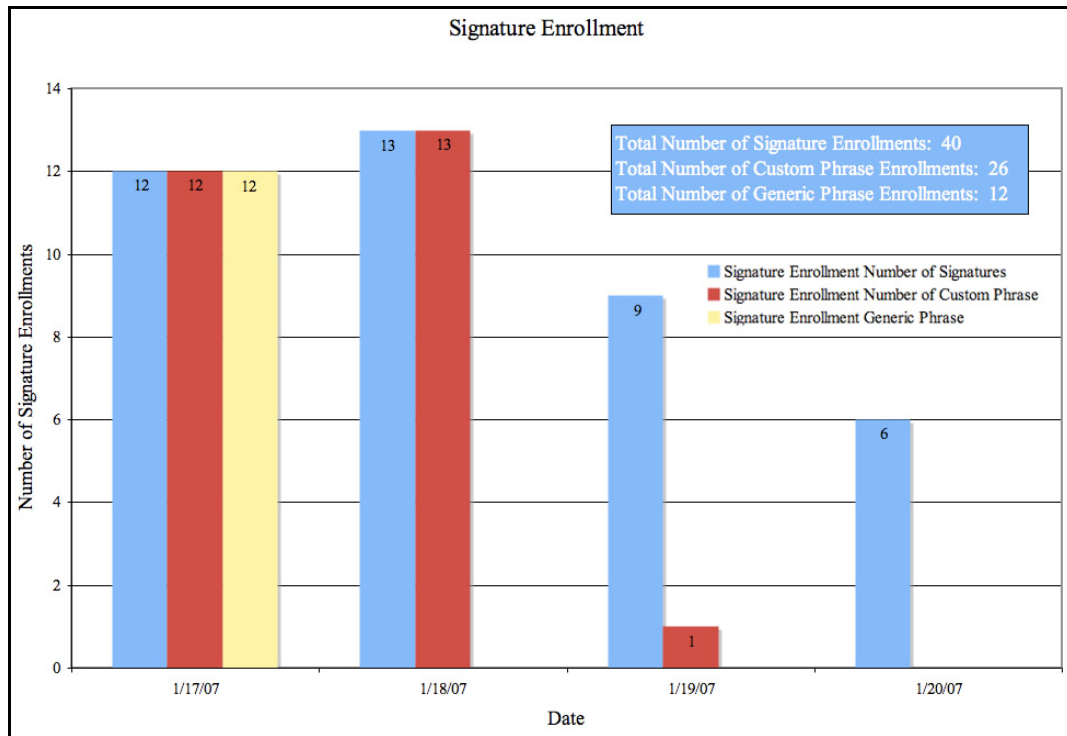


Figure 24. Signature Enrollment Report

Figure 25 presents the aggregate signature verification data, consisting of 192 verification attempts during the test phase. Figure 26 presents the verification attempts per signature model (User). Note that in Figure 26, several users had a very small number of verification attempts compared to others for a total of 192 signature verification attempts in the dataset. Due to privacy related issues, imposter trials were not conducted within this set of data. In a subsequent analysis, separate imposter testing was performed to determine the FRR and FAR of this system.

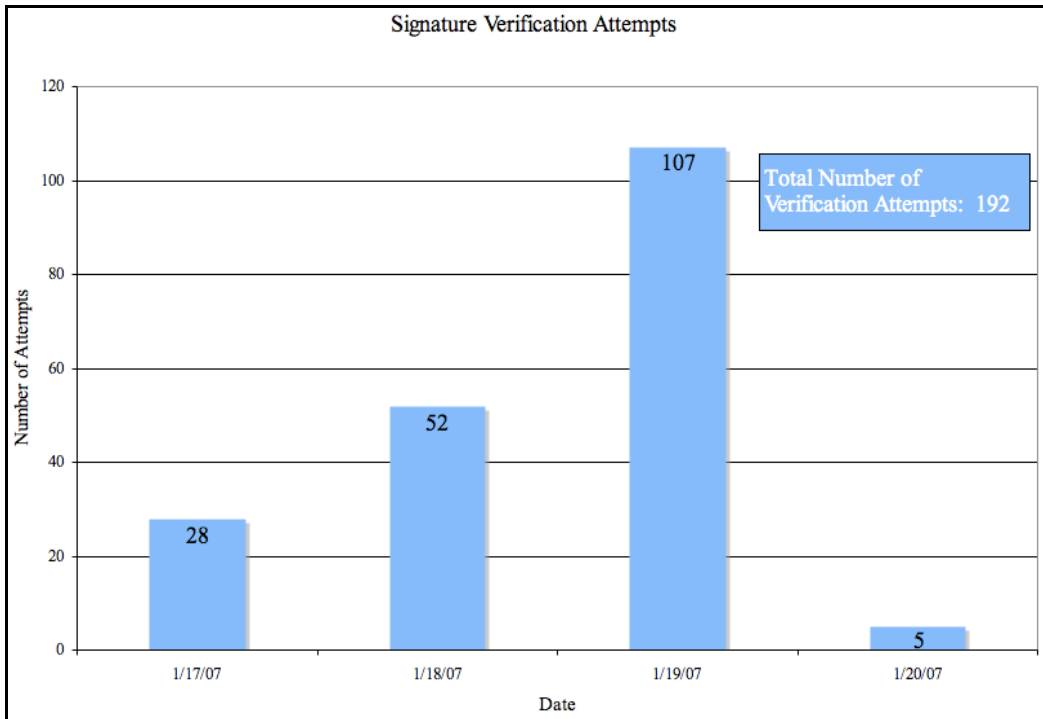


Figure 25. Signature Verification Report

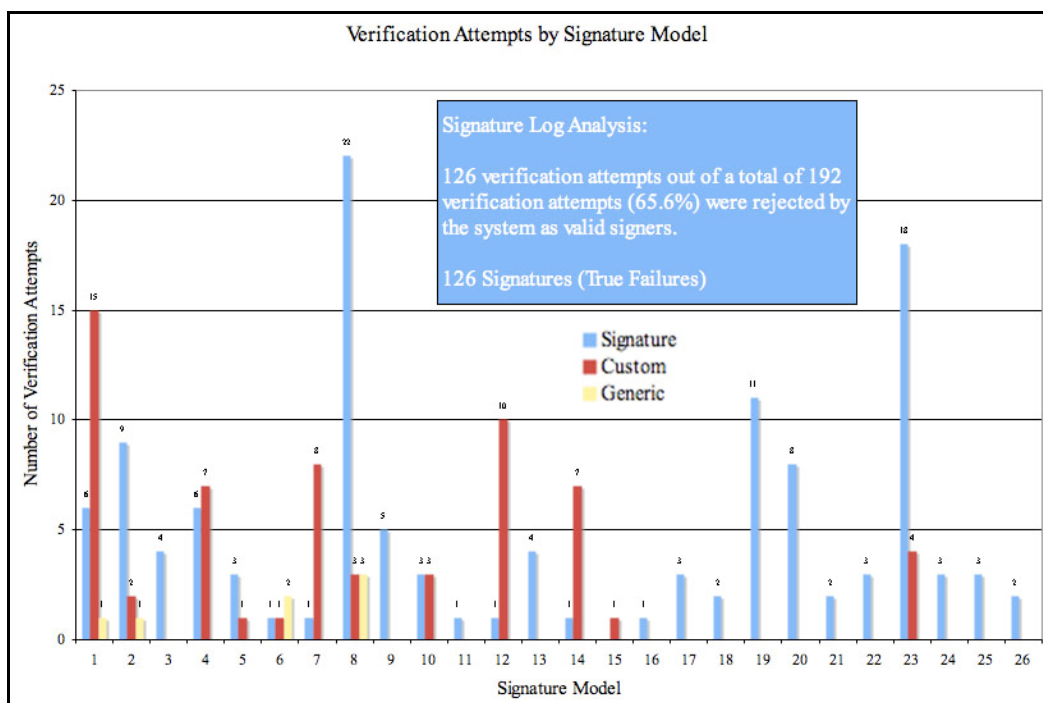


Figure 26. Number of Verification Attempts per Signature Model (User) Report

2. Imposter Test Analysis

Upon completion of the COASTS Signature Verification Test, two fictitious user IDs were created in order to perform an imposter test on the system. Imposters were given observation privileges (worst-case scenario) prior to attempting a false verification. Figure 27 presents the aggregate imposter data, consisting of the user “Billy Bob” and “User X”.

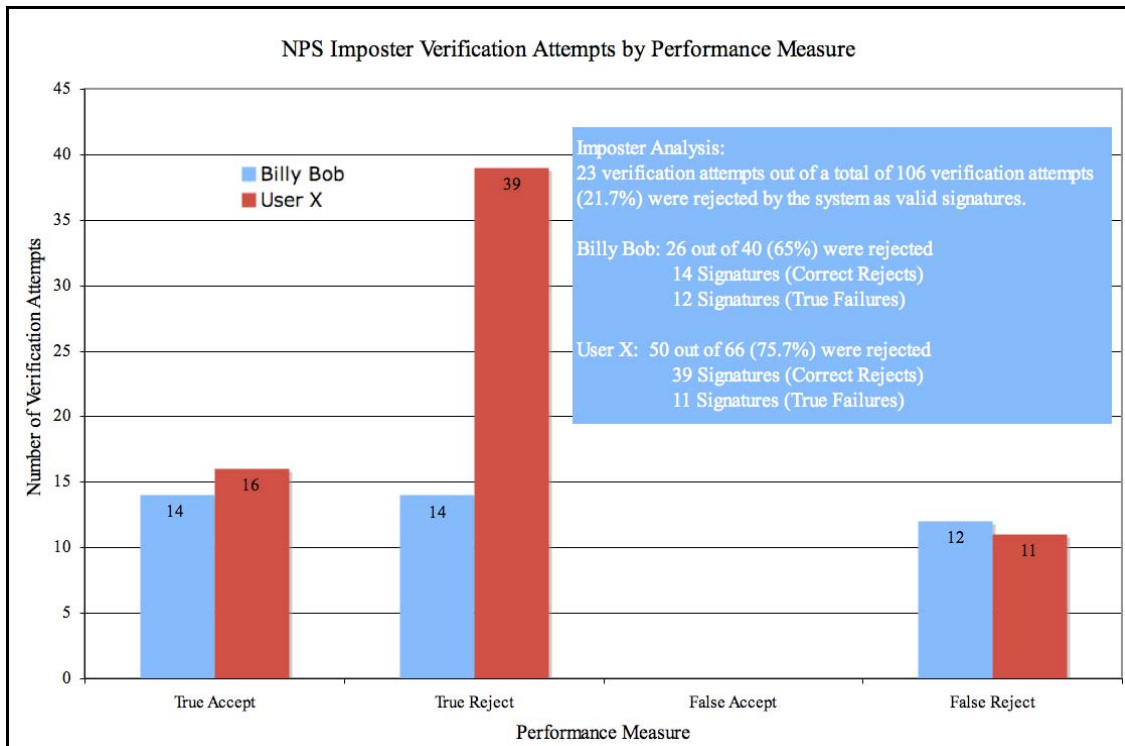


Figure 27. Number of Imposter Verification Attempts by Performance Measure

The user enrollments were performed by an individual familiar with the Bio-Pen® and had been using it with some frequency. Since the enrollments were made with a signature unfamiliar to the user, it is expected that there would be more false rejections due to the lack of experience with the fictitious signatures.

3. Comparison Analysis

Due to the limits of this test, construction of ROC curves would not be beneficial to the understanding of the results. Also, due to the lack of any false accepts, the ROC

curve would collapse into a line on a single axis. For better understanding of the data, a single data-point analysis was used to substitute a ROC curve analysis. In the context of the single data-point analysis, NPS defines the total number of valid verification attempts as:

$$NT = NTAR + NFRR + NFAR + NTFR.$$

where,

NT	The total number of valid verification attempts
NTAR	The total number of true accepts
NFRR	The total number of false rejects
NFAR	The total number of false accepts
NTFR	The total number of true failures

$$\text{False Reject Rate (FRR)} = NFRR / NT$$

$$\text{False Accept Rate (FAR)} = NFAR / NT$$

$$\begin{aligned} \text{Accuracy of the System} &= (NT - (NFRR + NFAR)) / NT \\ &= (NTAR + NTFR) / NT \end{aligned}$$

See Table 3 for a comparison of the NPS analysis versus the NPS imposter test.

DISCUSSION ITEM	NPS ANALYSIS (SIGNATURE)	NPS ANALYSIS (CUSTOM PHRASE)	NPS ANALYSIS (IMPOSTER TEST)
1. Enrollment	Total Signature Enrollment: 40	Total Signature Enrollment: 26	Total Signature Enrollment: 2
2. Total Number of Rejected Signatures	Total Nbr of Rejected Signatures: 81 (no imposter attempts)	Total Nbr of Rejected Signatures: 40 (no imposter attempts)	Total Nbr of Rejected Signatures: 76 Correct Rejects: 53 True Failures: 23
3. Valid Verification Attempts	Valid Verification Attempts: 123	Valid Verification Attempts: 62	Valid Verification Attempts: 106
4. True Failures	True Failures: 81	True Failures: 40	True Failures: 23
5. False Acceptance	False Acceptance: 0	False Acceptance: 0	False Acceptance: 0
6. Accuracy Analysis	FRR = 65.8% FAR = 0.0% Accuracy = 34.2%	FRR = 64.5% FAR = 0.0% Accuracy = 35.5%	FRR = 21.7% FAR = 0.0% Accuracy = 78.3%
<p>For the NPS Analysis of both the signature and custom phrase, it can be determined that familiarity with what a user is writing, whether it is their signature or a phrase of their own choosing, have an equal system accuracy. This expands the level of use for the pen beyond that of a signature alone.</p> <p>When the imposter test was conducted, there were more verification attempts on the two registration templates than on any other enrollment. This resulted in a more precise measure of the data in terms of system accuracy.</p> <p>Note: The testing did not allow enough time for users to be comfortable and familiar with the pen. The Bio-Pen System is designed to enhance the familiarity of the signature and the pen with each use. Thereby, the accuracy of the system will increase over time as the users continue to perform their signature.</p>			

Table 3. NPS COASTS Signature Verification Test Analysis Comparison

F. TEST LIMITATIONS

For purposes of this test, participants were expected to be who they claimed to be and hence no separate and independent identity checks were planned, either during or prior to registration. Furthermore, in this test, participation varied due to the level of preoccupation with other testing in COASTS. Also, the duration of the testing was shorter than desired.

Another variable of this test was the number of test subjects. The total number of signature enrollments was 40 participants; however, only 25 out of the 40 participants who initially registered made subsequent verification attempts with their signature biometrics. It would have been preferable to have at least 100 registrations and at least a thousand signature verification attempts.

Given the limited scope of this test, gauging how the error rates will scale up for the signature verification technology as the total amount of users grows is difficult. Due to the recent developments in signature verification as a biometric, no statistics are available with which to compare the data collected. Nor is it clear what the error rates and accuracy would be for consistent, frequent users of the Bio-Pen® system. Presently, the users are required to submit a user name when verifying their identity since no database look-up function exists.

G. SUMMARY

NPS successfully conducted a signature verification test to assess DynaSig's Bio-Pen® signature verification technology based on the performance measures of the FRR and FAR. During the test, COASTS did not impose any restrictions on the participants in terms of the writing surface used or which tip (ink or plastic) was used with the Bio-Pen®. For this particular data set, there were zero false acceptances recorded for the system. However, the adverse affect of the results was the large number of false rejections within the data. While the COASTS Test II signature verification testing yields a system accuracy of 34.2% for signatures and 35.5% for custom phrases, the imposter testing yields a system accuracy of 78.3%. The difference between the testing lies in the familiarity of the users to the Bio-Pen® and the importance of signature consistency. Further imposter testing is required with a greater number of participants that are familiar with the Bio-Pen® in order to more precisely determine system accuracy and if possible, perform a ROC curve analysis.

VI. CONCLUSION AND RECOMMENDATIONS

A. SUMMARY DISCUSSION

A need exists for increased security and control with regards to identity management. Many current biometric methods seek to provide a solution for this need, while newer biometric methods, such as dynamic signature verification, are emerging to address these identity management issues. After completion of this research, dynamic signature verification has been determined to be a viable form of biometric technology and merits further research. Dynamic signature biometrics offers unique capabilities that are unequaled in terms of the flexibility of the biometric, form factor, security and cost effectiveness. First, signature biometrics relies on an input that is natural, unobtrusive to produce, and already one of the most accepted methods of legal verification. Second, signature biometrics is language independent and can be used with any consistent, repeatable motion of the pen that reduces overall language translation costs. Third, signature biometrics increases the level of security through continuous use, much the opposite of traditional security measures.

This thesis has documented the results of the NPS signature verification test performed in conjunction with the COASTS field-testing. The intent of this project was to perform an initial evaluation of the DynaSig Bio-Pen® through research and a limited testing requirement. The NPS test, while showing the lack of any false acceptances, produced more than an acceptable amount of false rejections. However, it is noted that while the system accuracy for this one test was rather low (compared to other biometrics), it is estimated that over an extended period of testing, the accuracy would increase as the FRR decreases.

B. RECOMMENDATIONS FOR FURTHER RESEARCH

Upon completion of the initial testing of the DynaSig Bio-Pen® Signature Verification System, it is evident that further research is required to determine the best threshold for use in military and law enforcement applications. Additionally, further testing is recommended as future versions of the Bio-Pen® (to include a wireless version)

and implementations of the signature verification software become available. The following is a list of recommended further studies for NPS students in support of this research:

- Develop a test to determine the optimal threshold to minimize both FAR and FRR.
- Conduct further testing to determine effectiveness and advantages of a wireless version of the Bio-Pen®.
- Conduct a cost-benefit analysis of the deployment of signature verification technology within DoD and Homeland Defense.
- Incorporate the Bio-Pen® System with another biometric in developing a multimodal system.

APPENDIX A. NPS SIGNATURE VERIFICATION TEST SUMMARY

Pen SN	UserID	Mode	LogDate	DataSize	Result
3100163	user1a	3	1/18/11 10:06:23	1352	RGPD/14/0/2.8/4.0/3.0/2.6/1.5
3100163	user1a	3	1/18/11 10:06:38	1400	RGCP/10/65/3.1/4.2/3.5/2.3/2.4
3100163	user1a	1	1/18/11 10:06:56	1544	PASS/11/64/3.1/4.8/3.0/2.7/2.2
3100163	user1a	1	1/18/11 10:07:34	1562	PASS/1/61/3.1/4.8/3.0/2.5/2.1
3100163	user1a	1	1/18/11 10:08:45	1676	DENI/-55/25/3.4/5.0/5.0/1.3/2.3
3100164	user1a	1	1/19/11 16:35:14	1674	DENI/-55/58/3.8/5.0/3.5/2.8/3.7
3100164	user1a	1	1/19/11 16:35:32	1594	PASS/1/56/3.2/5.0/3.5/2.0/2.2
3100159	user1a	1	1/20/11 10:44:32	1340	PASS/1/79/3.1/4.0/3.0/2.6/2.8
3100163	user1b	3	1/18/11 10:09:45	1310	RGPD/14/0/2.7/3.9/3.0/1.1/2.8
3100163	user1b	3	1/18/11 10:09:58	1336	RGCF/15/66/2.6/4.0/2.5/1.3/2.6
3100163	user1b	1	1/18/11 10:10:13	1512	RGIC/-55/55/2.9/4.7/3.0/1.4/2.6
3100163	user1b	3	1/18/11 10:10:44	1404	RGPD/14/0/2.9/4.2/3.0/1.5/3.1
3100163	user1b	3	1/18/11 10:10:59	1374	RGCF/15/72/2.8/4.1/3.0/1.5/2.5
3100163	user1b	1	1/18/11 10:11:11	1380	RGIC/-55/55/2.5/4.1/2.5/1.2/2.3
3100163	user1b	3	1/18/11 10:12:32	1534	RGPD/14/0/3.4/4.7/5.0/2.0/2.1
3100163	user1b	3	1/18/11 10:12:49	1386	RGCP/10/59/3.3/4.2/5.0/1.5/2.4
3100163	user1b	1	1/18/11 10:13:03	1434	PASS/12/73/3.3/4.4/5.0/1.6/2.3
3100163	user1c	3	1/18/11 10:15:17	1398	RGPD/14/0/3.3/4.2/5.0/1.7/2.3
3100163	user1c	3	1/18/11 10:15:29	1448	RGCP/10/63/3.3/4.4/5.0/2.1/1.7
3100163	user1c	1	1/18/11 10:15:45	1404	PASS/12/61/3.3/4.2/5.0/2.2/1.8
3100164	user1c	1	1/19/11 16:36:16	1574	DENI/-55/35/3.6/4.9/5.0/2.2/2.5
3100164	user1c	1	1/19/11 16:36:38	500	DENI/-55/0/1.4/0.8/1.5/1.6/1.7
3100164	user1c	1	1/19/11 16:36:55	1566	DENI/-55/28/3.5/4.9/5.0/2.2/1.9
3100164	user1c	1	1/19/11 16:37:13	1524	DENI/-55/49/3.8/4.7/5.0/2.6/3.0
3100164	user1c	1	1/19/11 16:39:41	1596	DENI/-55/0/3.2/5.0/5.0/2.8/0.0
3100164	user1c	1	1/19/11 16:40:08	1444	DENI/-55/0/3.0/4.4/5.0/2.8/0.0
3100164	user1c	1	1/19/11 16:40:40	1348	SVBS/444
3100164	user1c	1	1/19/11 16:40:58	1458	DENI/-55/32/3.5/4.4/5.0/2.6/2.1
3100164	user1c	1	1/19/11 16:41:13	1476	DENI/-55/57/4.2/4.5/5.0/3.2/4.0
3100164	user1c	1	1/19/11 16:41:29	1386	DENI/-55/29/3.3/4.2/3.0/2.7/3.5
3100164	user1c	1	1/19/11 16:41:49	1422	FLAG/4/52/4.0/4.3/5.0/3.1/3.4
3100164	user1c	1	1/19/11 16:42:05	1578	DENI/-55/53/4.1/4.9/5.0/2.9/3.7
3100164	user1c	1	1/19/11 16:42:20	1528	DENI/-55/22/3.6/4.7/5.0/1.9/2.9
3100164	user1c	1	1/19/11 16:44:43	1570	DENI/-55/36/3.6/4.9/5.0/1.9/2.7
3100159	user1c	1	1/20/11 10:45:14	1596	PASS/1/61/4.0/5.0/5.0/3.4/2.6
3100156	user2a	3	1/18/11 10:37:22	870	RGPD/14/0/2.9/2.2/2.5/3.9/3.0

Pen SN	UserID	Mode	LogDate	DataSize	Result
3100156	user2a	3	1/18/11 10:37:37	896	RGCP/10/61/2.9/2.3/2.5/4.2/2.6
3100156	user2a	1	1/18/11 10:37:56	890	PASS/12/83/3.3/2.3/2.5/4.5/3.9
3100161	user2a	1	1/19/11 11:12:04	838	DENI/-55/37/2.3/2.1/1.5/3.5/2.1
3100161	user2a	1	1/19/11 11:12:17	928	DENI/-55/48/2.7/2.4/2.0/3.5/2.8
3100156	user2a	1	1/19/11 11:12:41	810	SVBS/444
3100156	user2a	1	1/19/11 11:12:56	920	DENI/-55/46/3.1/2.4/3.0/3.1/3.8
3100156	user2a	1	1/19/11 11:13:41	932	DENI/-55/43/2.9/2.4/2.5/3.0/3.6
3100156	user2a	1	1/19/11 11:13:57	1024	DENI/-55/48/3.4/2.8/3.5/3.2/4.0
3100156	user2a	1	1/19/11 12:13:53	876	FLAG/4/62/2.9/2.2/3.5/2.2/3.7
3100156	user2a	1	1/19/11 12:14:05	910	DENI/-55/45/2.6/2.3/3.5/2.5/2.2
3100156	user2a	3	1/19/11 12:19:51	850	RGPD/14/0/2.4/2.1/3.0/1.7/2.8
3100156	user2a	3	1/19/11 12:20:01	886	RGOM/-60/40/2.7/2.2/3.5/2.6/2.5
3100156	user2a	3	1/19/11 12:20:13	894	RGCP/12/80/2.9/2.3/3.5/2.8/2.8
3100156	user2a	1	1/19/11 12:20:35	888	PASS/12/84/3.1/2.3/3.5/3.1/3.7
3100156	user2b	3	1/18/11 10:38:37	1080	RGPD/14/0/3.4/3.0/2.5/3.9/4.1
3100156	user2b	3	1/18/11 10:38:49	1070	RGOM/-60/45/3.3/3.0/2.0/4.0/4.1
3100156	user2b	3	1/18/11 10:39:01	1232	RGCP/11/56/3.6/3.6/2.5/4.4/4.1
3100156	user2b	1	1/19/11 11:14:38	1228	DENI/-55/21/3.7/3.6/5.0/2.6/3.7
3100156	user2c	3	1/18/11 10:39:42	820	RGPD/14/0/2.3/2.0/2.0/3.3/1.9
3100156	user2c	3	1/18/11 10:39:55	782	RGCF/15/83/2.8/1.8/2.0/4.1/3.1
3100156	user2c	1	1/18/11 10:40:07	790	RGCP/11/89/2.8/1.9/2.0/3.5/3.6
3100156	user2c	1	1/18/11 10:40:28	778	PASS/12/91/3.0/1.8/2.0/4.5/3.5
3100156	user2c	1	1/19/11 11:14:11	852	DENI/-55/57/2.7/2.1/2.5/2.8/3.5
3100156	user3a	3	1/18/11 10:44:55	710	RGPD/14/0/2.5/1.6/1.5/5.0/2.0
3100156	user3a	3	1/18/11 10:45:05	702	RGCP/10/68/2.9/1.5/1.5/4.6/4.0
3100156	user3a	1	1/18/11 10:45:35	620	DENI/-55/0/1.5/1.2/1.5/0.0/3.2
3100156	user3a	1	1/18/11 10:45:45	100	DENI/-55/0/1.1/0.0/0.0/4.5/0.0
3100156	user3a	1	1/18/11 10:45:54	656	DENI/-55/0/1.7/1.4/1.5/9.0/3.8
3100156	user3a	1	1/18/11 10:46:10	610	PASS/12/54/2.8/1.2/1.5/4.9/3.5
3100156	user3b	3	1/18/11 10:46:44	1080	RGPD/14/0/3.8/3.0/5.0/4.5/2.8
3100156	user3b	3	1/18/11 10:46:55	1120	RGCP/10/62/4.0/3.1/5.0/4.6/3.1
3100156	user3c	3	1/18/11 10:47:49	612	RGPD/14/0/3.2/1.2/3.0/4.8/3.7
3100156	user3c	3	1/18/11 10:48:00	582	RGCP/10/80/3.0/1.1/3.0/4.6/3.2
3100156	user4a	3	1/18/11 10:49:44	1596	RGPD/14/0/3.6/5.0/1.5/4.1/3.8
3100156	user4a	3	1/18/11 10:50:02	1480	RGCP/10/78/3.3/4.5/1.5/3.4/3.7
3100156	user4a	1	1/19/11 12:02:14	1274	DENI/-55/44/3.1/3.7/3.5/1.7/3.5
3100156	user4a	1	1/19/11 12:02:34	1450	DENI/-55/53/3.0/4.4/3.0/2.1/2.4
3100156	user4a	1	1/19/11 12:02:47	1460	DENI/-55/44/3.3/4.5/5.0/1.7/2.0
3100156	user4a	1	1/19/11 12:03:09	1408	FLAG/4/63/2.8/4.3/2.0/2.4/2.5
3100156	user4a	1	1/19/11 12:03:23	1450	PASS/11/66/2.7/4.4/1.5/2.4/2.3

Pen SN	UserID	Mode	LogDate	DataSize	Result
3100159	user4a	1	1/20/11 14:55:49	1404	PASS/1/69/2.9/4.2/1.5/2.7/3.1
3100156	user4b	3	1/18/11 10:50:52	1424	RGPD/14/0/2.8/4.3/0.5/2.8/3.4
3100156	user4b	3	1/18/11 10:51:05	1322	RGCP/10/53/2.7/3.9/0.5/3.1/3.4
3100156	user4c	3	1/18/11 10:52:09	1264	RGPD/14/0/3.2/3.7/4.0/2.3/2.9
3100156	user4c	3	1/18/11 10:52:21	1322	RGCP/10/64/3.3/3.9/4.0/1.8/3.4
3100156	user4c	1	1/19/11 12:04:08	948	FLAG/4/47/2.8/2.5/4.0/2.8/2.0
3100156	user4c	1	1/19/11 12:04:18	1066	PASS/11/57/3.1/2.9/4.0/2.4/2.9
3100159	user4c	1	1/20/11 14:56:35	1146	PASS/1/75/3.2/3.2/4.0/2.4/3.4
3100161	user4c	1	1/20/11 14:57:44	1036	DENI/-55/0/2.2/2.8/4.0/1.9/0.0
3100161	user4c	1	1/20/11 14:57:59	1180	DENI/-55/0/2.2/3.4/4.0/1.2/0.0
3100161	user4c	1	1/20/11 14:58:10	1146	DENI/-55/0/2.3/3.2/4.0/1.8/0.0
3100161	user4c	1	1/20/11 14:58:26	980	PASS/1/58/2.9/2.6/4.0/1.7/3.4
3100156	user5a	3	1/18/11 11:24:42	968	RGPD/14/0/2.9/2.6/3.0/2.8/3.2
3100161	user5a	3	1/18/11 11:25:38	1070	RGPD/14/0/2.4/3.0/1.5/1.8/3.4
3100161	user5a	3	1/18/11 11:25:52	1234	RGOM/-60/40/2.9/3.6/3.0/2.1/3.1
3100161	user5a	3	1/18/11 11:26:10	1044	RGCP/11/63/2.6/2.9/1.5/2.4/3.5
3100161	user5a	1	1/18/11 11:26:40	922	DENI/-55/49/2.2/2.4/2.0/2.2/2.4
3100161	user5a	1	1/18/11 11:26:59	238	DENI/-55/0/1.3/0.0/0.0/2.3/2.9
3100161	user5a	1	1/18/11 11:27:18	1042	PASS/11/60/2.5/2.8/2.0/2.6/2.7
3100161	user5b	3	1/18/11 11:30:01	1012	RGPD/14/0/2.8/2.7/4.5/2.2/1.9
3100161	user5b	3	1/18/11 11:30:35	1388	RGOM/-60/0/3.6/4.2/5.0/2.0/3.2
3100161	user5b	3	1/18/11 11:30:45	1004	RGCP/11/60/2.9/2.7/4.5/2.2/2.2
3100161	user5c	3	1/18/11 11:31:47	580	RGPD/14/0/1.8/1.1/2.0/2.2/2.1
3100161	user5c	3	1/18/11 11:32:04	612	RGOM/-60/37/2.0/1.2/2.0/2.2/2.5
3100161	user5c	3	1/18/11 11:32:15	606	FLAG/4/49/2.0/1.2/2.0/2.1/2.5
3100161	user5c	1	1/18/11 11:32:34	750	DENI/-55/5/2.5/1.7/3.0/2.1/3.0
3100161	user5d	3	1/18/11 11:33:07	610	RGPD/14/0/1.6/1.2/1.0/2.4/1.9
3100161	user5d	3	1/18/11 11:33:18	588	RGOM/-60/37/1.5/1.1/0.5/2.4/1.9
3100161	user5d	3	1/18/11 11:33:26	554	RGIC/-55/0/1.4/1.0/0.0/2.4/2.3
3100161	user5d	3	1/18/11 11:33:44	534	DISC/-58/0/1.2/0.9/0.0/2.3/1.5
3100161	user5d	3	1/18/11 11:34:07	526	DISC/-58/0/0.7/0.9/0.0/1.8/0.0
3100161	user5d	3	1/18/11 11:34:25	516	RGPD/14/0/1.8/0.8/2.0/1.9/2.5
3100161	user5d	3	1/18/11 11:34:33	530	RGCP/10/76/2.1/0.9/2.0/2.1/3.5
3100161	user5d	1	1/18/11 11:34:58	508	PASS/11/87/2.1/0.8/2.0/2.3/3.5
3100163	user6a	3	1/18/11 12:02:02	658	RGPD/14/0/2.2/1.4/1.0/3.5/2.8
3100163	user6a	3	1/18/11 12:02:11	584	RGCP/10/59/1.9/1.1/1.0/3.0/2.5
3100163	user6a	1	1/18/11 12:02:38	598	PASS/12/73/2.3/1.1/1.0/4.0/3.0
3100163	user6b	3	1/18/11 12:03:16	1078	RGPD/14/0/2.6/3.0/1.0/3.7/2.7
3100163	user6b	3	1/18/11 12:03:26	1100	RGCF/15/67/2.2/3.1/0.5/3.7/1.7
3100163	user6b	1	1/18/11 12:03:40	934	RGCP/11/56/2.1/2.4/1.0/3.4/1.6

Pen SN	UserID	Mode	LogDate	DataSize	Result
3100163	user6b	1	1/18/11 12:06:33	794	DENI/-55/44/1.8/1.9/0.5/1.6/3.2
3100163	user6b	1	1/18/11 12:06:44	964	DENI/-55/58/1.8/2.5/0.5/1.5/2.5
3100163	user6c	3	1/18/11 12:04:33	1316	RGPD/14/0/3.1/3.9/3.5/2.8/2.4
3100163	user6c	3	1/18/11 12:04:42	814	RGOM/-60/0/2.1/2.0/2.0/2.5/2.1
3100163	user6c	3	1/18/11 12:04:53	1014	RGIC/-55/51/2.8/2.7/3.0/2.0/3.5
3100163	user6c	3	1/18/11 12:05:17	882	RGPD/14/0/2.0/2.2/2.5/1.3/1.8
3100163	user6c	3	1/18/11 12:05:26	814	RGCF/15/77/2.1/2.0/2.5/1.6/2.4
3100163	user6c	1	1/18/11 12:05:36	812	RGCP/12/87/2.3/2.0/2.5/1.8/2.8
3100163	user6c	1	1/18/11 12:06:56	818	PASS/11/73/2.3/2.0/2.5/1.6/3.1
3100156	user7a	3	1/18/11 12:24:55	1222	RGPD/14/0/3.6/3.5/3.0/4.9/2.9
3100156	user7a	3	1/18/11 12:25:07	1220	RGOM/-60/0/2.6/3.5/3.0/9.0/3.8
3100156	user7a	3	1/18/11 12:25:21	1156	RGCP/12/63/3.7/3.3/2.5/4.8/4.0
3100156	user7b	3	1/18/11 12:26:11	1238	RGPD/14/0/3.5/3.6/3.5/3.4/3.6
3100156	user7b	3	1/18/11 12:26:24	1282	RGOM/-60/17/3.8/3.8/3.0/4.1/4.3
3100156	user7b	3	1/18/11 12:26:38	1286	RGCP/11/60/3.7/3.8/3.5/4.1/3.4
3100156	user7c	3	1/18/11 12:27:24	970	RGPD/14/0/2.8/2.6/2.0/3.7/3.0
3100156	user7c	3	1/18/11 12:27:35	1024	RGCF/15/64/2.9/2.8/2.0/3.9/3.2
3100156	user7c	1	1/18/11 12:27:49	1040	RGCP/11/60/3.1/2.8/2.5/4.4/2.8
3100161	user8a	3	1/18/11 12:32:36	508	RGPD/14/0/1.7/0.8/1.0/2.9/2.0
3100161	user8a	3	1/18/11 12:32:45	476	RGCP/10/67/2.0/0.7/1.0/3.5/2.9
3100161	user8a	1	1/18/11 12:33:07	482	PASS/12/79/2.2/0.7/1.0/3.6/3.6
3100161	user8b	3	1/18/11 12:33:53	1062	RGPD/14/0/3.4/2.9/4.5/3.1/3.3
3100161	user8b	3	1/18/11 12:34:10	992	RGOM/-60/36/3.6/2.7/4.5/3.5/3.6
3100161	user8b	3	1/18/11 12:34:21	1148	RGIC/-55/34/3.7/3.3/5.0/3.8/2.8
3100161	user8b	3	1/18/11 12:34:53	1300	RGPD/14/0/3.6/3.8/4.5/4.0/2.1
3100161	user8b	3	1/18/11 12:35:06	1372	RGOM/-60/0/3.2/4.1/4.5/4.1/0.0
3100161	user8b	3	1/18/11 12:35:18	1378	RGCP/12/71/3.6/4.1/4.5/4.2/1.7
3100161	user8c	3	1/18/11 12:36:34	1318	RGPD/14/0/3.1/3.9/2.0/4.6/2.0
3100161	user8c	3	1/18/11 12:36:45	1268	RGOM/-60/37/3.1/3.7/1.5/5.0/2.3
3100161	user8c	3	1/18/11 12:36:55	1086	RGIC/-55/50/3.1/3.0/2.0/4.7/2.7
3100161	user8c	3	1/18/11 12:37:22	1170	RGPD/14/0/3.2/3.3/3.5/3.9/2.2
3100161	user8c	3	1/18/11 12:37:32	1186	RGOM/-60/47/4.0/3.4/4.5/4.1/3.8
3100161	user8c	3	1/18/11 12:37:43	1390	RGCP/11/54/3.8/4.2/3.5/4.2/3.3
3100161	user8c	1	1/18/11 12:38:56	1096	FLAG/4/54/3.9/3.1/4.5/4.1/3.8
3100161	user8c	1	1/18/11 12:39:09	1244	PASS/12/57/4.0/3.6/4.5/4.2/3.7
3100161	user8c	1	1/19/11 14:08:16	1276	FLAG/4/50/3.4/3.7/4.5/2.7/2.6
3100161	user8c	1	1/19/11 14:08:28	1242	FLAG/4/50/3.4/3.6/4.5/3.2/2.4
3100161	user8c	1	1/19/11 14:08:40	1346	FLAG/4/47/3.5/4.0/4.5/2.9/2.7
3100161	user8c	1	1/19/11 14:08:53	1296	PASS/4/50/3.6/3.8/4.5/3.7/2.4
3100161	user8c	1	1/19/11 14:13:44	1114	PASS/1/58/3.1/3.1/3.5/3.4/2.3

Pen SN	UserID	Mode	LogDate	DataSize	Result
3100161	user8d	3	1/18/11 12:40:08	640	DISC/-58/0/2.0/1.3/2.5/4.4/0.0
3100161	user8d	3	1/18/11 12:40:19	594	DISC/-58/0/1.9/1.1/2.5/4.1/0.0
3100161	user8d	3	1/18/11 12:40:47	556	DISC/-58/0/1.8/1.0/2.5/3.7/0.0
3100161	user8d	3	1/18/11 12:41:16	628	DISC/-58/0/2.1/1.3/3.5/3.7/0.0
3100161	user8d	3	1/18/11 12:42:00	1188	RGPD/14/0/2.8/3.4/1.5/4.3/1.9
3100161	user8d	3	1/18/11 12:42:11	1206	RGOM/-60/0/2.2/3.5/1.5/3.9/0.0
3100161	user8d	3	1/18/11 12:42:21	1142	RGCP/11/78/2.6/3.2/1.5/4.0/1.6
3100161	user8d	1	1/19/11 14:14:17	990	PASS/11/67/2.3/2.6/1.5/3.5/1.5
3100161	user9a	3	1/18/11 15:40:32	528	RGPD/14/0/2.0/0.9/2.5/2.8/1.7
3100161	user9a	3	1/18/11 15:40:51	556	RGOM/-60/54/2.6/1.0/3.0/3.3/3.1
3100161	user9a	3	1/18/11 15:41:35	544	RGCP/11/69/2.1/0.9/2.5/2.4/2.8
3100161	user9a	1	1/20/11 11:34:58	532	DENI/-55/0/1.8/0.9/2.0/4.3/0.0
3100161	user9a	1	1/20/11 11:35:07	556	FLAG/4/61/2.1/1.0/1.5/4.4/1.5
3100161	user9a	1	1/20/11 11:35:17	514	DENI/-55/44/2.2/0.8/2.0/4.5/1.7
3100161	user9a	1	1/20/11 11:35:26	594	DENI/-55/44/2.5/1.1/3.0/4.1/1.9
3100161	user9a	1	1/20/11 11:35:45	512	DENI/-55/30/2.1/0.8/2.0/3.7/1.9
3100161	user9a	1	1/20/11 11:35:54	536	DENI/-55/48/2.0/0.9/1.5/2.8/3.0
3100161	user9a	1	1/20/11 11:36:05	622	DENI/-55/53/2.4/1.2/2.5/3.0/2.8
3100161	user9a	1	1/20/11 11:36:18	612	DENI/-55/51/2.2/1.2/1.5/3.7/2.5
3100161	user9a	1	1/20/11 11:36:25	598	DENI/-55/37/2.1/1.1/1.5/3.0/2.9
3100159	user9a	1	1/20/11 11:36:50	604	DENI/-55/41/1.9/1.2/1.5/3.9/1.0
3100159	user9a	1	1/20/11 11:37:00	660	DENI/-55/39/2.4/1.4/2.0/4.1/2.3
3100159	user9a	1	1/20/11 11:37:08	644	DENI/-55/24/2.2/1.3/1.5/4.1/1.8
3100161	user9a	1	1/20/11 11:38:52	640	DENI/-55/23/2.5/1.3/3.0/3.2/2.3
3100161	user9a	1	1/20/11 11:39:07	616	DENI/-55/46/2.5/1.2/2.5/3.8/2.7
3100161	user9a	1	1/20/11 11:41:00	662	DENI/-55/32/2.4/1.4/1.5/3.5/3.4
3100161	user9a	1	1/20/11 11:41:09	700	DENI/-55/27/2.8/1.5/2.0/3.9/3.6
3100161	user9a	1	1/20/11 11:41:26	628	DENI/-55/29/2.6/1.3/2.0/3.5/3.4
3100161	user9a	1	1/20/11 11:41:46	614	DENI/-55/34/2.4/1.2/1.5/3.9/2.9
3100161	user9a	1	1/20/11 11:41:55	680	DENI/-55/40/2.3/1.5/1.5/3.2/3.1
3100161	user9a	1	1/20/11 11:42:03	562	DENI/-55/33/2.5/1.0/2.0/3.9/3.1
3100161	user9a	1	1/20/11 11:42:20	628	DENI/-55/20/2.2/1.3/1.5/4.2/1.9
3100161	user9a	1	1/21/11 16:07:41	566	DENI/-55/50/2.0/1.0/2.5/1.7/2.7
3100161	user9b	3	1/18/11 15:42:28	1352	RGPD/14/0/3.1/4.0/5.0/1.1/2.2
3100161	user9b	3	1/18/11 15:42:41	1492	RGCF/15/58/3.6/4.6/5.0/1.4/3.4
3100161	user9b	1	1/18/11 15:42:54	1460	RGCP/12/70/3.5/4.5/5.0/1.4/3.1
3100161	user9b	1	1/20/11 11:37:38	1612	DENI/-55/29/3.8/5.0/5.0/1.9/3.3
3100161	user9b	1	1/20/11 11:37:51	1442	DENI/-55/34/3.6/4.4/5.0/2.7/2.4
3100161	user9b	1	1/20/11 11:38:03	1408	PASS/11/66/3.6/4.3/5.0/2.5/2.8
3100161	user9c	3	1/18/11 15:43:48	792	RGPD/14/0/2.2/1.9/3.0/0.9/2.9

Pen SN	UserID	Mode	LogDate	DataSize	Result
3100161	user9c	3	1/18/11 15:43:57	798	RGOM/-60/37/2.3/1.9/3.5/1.0/2.7
3100161	user9c	3	1/18/11 15:44:07	854	RGCP/11/67/2.0/2.1/3.0/1.1/1.9
3100161	user9c	1	1/20/11 11:45:38	876	DENI/-55/53/2.9/2.2/3.5/1.8/4.2
3100161	user9c	1	1/20/11 11:45:49	918	DENI/-55/38/2.7/2.4/3.5/1.3/3.5
3100161	user9c	1	1/20/11 11:46:06	862	PASS/11/64/2.8/2.2/3.5/1.6/3.8
3100161	user10a	3	1/18/11 16:08:28	676	RGPD/14/0/1.8/1.4/1.5/2.3/2.1
3100161	user10a	3	1/18/11 16:08:41	704	RGOM/-60/43/1.4/1.5/0.5/1.8/1.6
3100161	user10a	3	1/18/11 16:08:51	652	RGIC/-55/2/1.7/1.3/0.5/1.8/3.2
3100161	user10a	3	1/18/11 16:09:09	616	DISC/-58/0/1.6/1.2/0.0/2.4/2.9
3100161	user10a	3	1/18/11 16:09:24	510	RGPD/14/0/1.7/0.8/0.5/2.5/3.0
3100161	user10a	3	1/18/11 16:09:37	488	RGOM/-60/24/1.7/0.7/0.5/2.3/3.3
3100161	user10a	3	1/18/11 16:09:48	608	RGIC/-55/19/1.8/1.2/1.0/1.8/3.2
3100161	user10a	3	1/18/11 16:10:05	1176	RGPD/14/0/2.3/3.4/0.5/2.1/3.3
3100161	user10a	3	1/18/11 16:10:18	620	RGOM/-60/0/1.7/1.2/1.0/1.4/3.3
3100161	user10a	3	1/18/11 16:10:27	436	RGIC/-55/42/1.5/0.5/1.0/1.9/2.5
3100161	user10a	3	1/18/11 16:11:00	120	DISC/-58/0/2.1/0.0/1.0/3.5/3.7
3100159	user10a	3	1/18/11 16:11:30	472	RGPD/14/0/1.8/0.7/1.5/1.7/3.4
3100159	user10a	3	1/18/11 16:11:40	544	RGOM/-60/46/1.6/0.9/1.0/1.9/2.7
3100159	user10a	3	1/18/11 16:11:49	576	RGCP/12/60/1.6/1.1/0.5/2.2/2.8
3100159	user10a	1	1/18/11 16:17:24	566	SVBS/444
3100159	user10a	1	1/18/11 16:17:39	666	DENI/-55/20/1.8/1.4/0.5/2.2/3.1
3100159	user10a	1	1/18/11 16:17:56	604	DENI/-55/0/1.7/1.2/0.0/2.3/3.5
3100159	user10a	1	1/18/11 16:18:23	880	DENI/-55/0/2.2/2.2/0.0/3.1/3.6
3100159	user10a	1	1/18/11 16:18:34	694	DENI/-55/0/2.2/1.5/0.0/3.7/3.4
3100159	user10a	1	1/18/11 16:18:45	596	PASS/12/55/1.8/1.1/0.5/2.5/3.0
3100159	user10b	3	1/18/11 16:12:43	1338	RGPD/14/0/3.4/4.0/5.0/2.1/2.5
3100159	user10b	3	1/18/11 16:12:57	1510	RGOM/-60/28/3.9/4.6/5.0/2.2/3.7
3100159	user10b	3	1/18/11 16:13:10	1496	RGIC/-55/36/4.0/4.6/5.0/2.9/3.4
3100159	user10b	3	1/18/11 16:13:43	1336	RGPD/14/0/3.9/4.0/5.0/3.6/3.0
3100159	user10b	3	1/18/11 16:13:56	1330	RGCF/15/58/4.0/4.0/5.0/3.4/3.4
3100159	user10b	1	1/18/11 16:14:09	1392	RGCP/12/63/4.0/4.2/5.0/3.4/3.4
3100159	user10c	3	1/18/11 16:15:50	254	DISC/-58/0/1.3/0.0/0.5/2.2/2.5
3100159	user10c	3	1/18/11 16:16:00	778	RGPD/14/0/2.2/1.8/3.0/1.8/2.2
3100159	user10c	3	1/18/11 16:16:11	830	RGCP/10/69/2.6/2.0/3.0/2.4/3.0
3100159	user11a	3	1/18/11 16:27:26	1230	RGPD/14/0/3.4/3.6/2.5/4.0/3.4
3100159	user11a	3	1/18/11 16:27:37	932	RGOM/-60/50/2.9/2.4/2.0/4.5/2.8
3100159	user11a	3	1/18/11 16:27:49	1110	RGCP/12/49/3.3/3.1/2.0/4.3/3.7
3100159	user11a	3	1/18/11 16:28:08	1068	RGPD/14/0/3.1/2.9/2.0/3.7/3.6
3100159	user11a	3	1/18/11 16:28:28	1052	RGOM/-60/36/3.1/2.9/2.0/4.1/3.4
3100159	user11a	3	1/18/11 16:28:47	832	RGCP/11/70/2.8/2.0/2.0/4.0/3.1

Pen SN	UserID	Mode	LogDate	DataSize	Result
3100159	user11b	3	1/18/11 16:30:58	884	RGPD/14/0/2.7/2.2/3.5/2.6/2.4
3100159	user11b	3	1/18/11 16:31:07	978	RGOM/-60/40/3.3/2.6/4.5/3.2/2.9
3100159	user11b	3	1/18/11 16:31:17	988	RGIC/-55/49/3.1/2.6/4.0/3.4/2.4
3100159	user11b	3	1/18/11 16:31:41	850	RGPD/14/0/2.9/2.1/3.5/3.4/2.5
3100159	user11b	3	1/18/11 16:31:56	816	RGOM/-60/37/3.0/2.0/3.5/3.5/2.9
3100159	user11b	3	1/18/11 16:32:05	814	RGIC/-55/47/2.4/2.0/2.0/3.4/2.4
3100159	user11b	3	1/18/11 16:32:21	838	RGPD/14/0/2.9/2.1/3.0/3.3/3.3
3100159	user11b	3	1/18/11 16:32:55	864	RGOM/-60/30/2.4/2.2/2.0/2.8/2.7
3100159	user11b	3	1/18/11 16:33:13	718	RGIC/-55/11/2.1/1.6/1.0/2.7/3.3
3100159	user11b	3	1/18/11 16:34:06	702	RGPD/14/0/2.1/1.5/0.5/3.2/3.0
3100159	user11b	3	1/18/11 16:34:16	758	RGOM/-60/30/2.5/1.8/2.0/2.9/3.5
3100159	user11b	3	1/18/11 16:34:27	658	RGIC/-55/39/2.1/1.4/1.0/3.3/2.8
3100159	user11b	3	1/18/11 16:34:39	354	DISC/-58/0/1.2/0.2/0.0/2.0/2.4
3100159	user11b	3	1/18/11 16:34:51	1166	RGPD/14/0/3.3/3.3/3.5/3.2/3.1
3100159	user11b	3	1/18/11 16:35:00	1182	RGOM/-60/41/3.7/3.4/4.5/3.3/3.6
3100159	user11b	3	1/18/11 16:35:10	1210	RGIC/-55/35/3.7/3.5/4.5/3.2/3.6
3100159	user11b	3	1/18/11 16:35:35	1112	RGPD/14/0/2.6/3.1/1.5/2.7/3.2
3100159	user11b	3	1/18/11 16:35:45	922	RGOM/-60/11/2.6/2.4/2.0/2.9/3.0
3100159	user11b	3	1/18/11 16:35:54	820	RGIC/-55/38/2.4/2.0/1.5/2.8/3.2
3100159	user11b	3	1/18/11 16:36:20	1288	RGPD/14/0/3.8/3.8/5.0/3.1/3.2
3100159	user11b	3	1/18/11 16:36:31	1342	RGCP/10/71/3.8/4.0/5.0/3.4/3.0
3100159	user11c	3	1/18/11 16:38:01	1412	RGPD/14/0/3.8/4.3/5.0/2.7/3.3
3100159	user11c	3	1/18/11 16:38:09	366	RGOM/-60/0/1.6/0.2/1.0/3.1/2.0
3100159	user11c	3	1/18/11 16:38:26	284	RGIC/-55/0/1.6/0.0/1.5/3.0/2.1
3100159	user11c	3	1/18/11 16:38:37	298	DISC/-58/0/1.7/0.0/1.5/3.0/2.1
3100159	user11c	3	1/18/11 16:39:56	536	RGPD/14/0/2.1/0.9/2.5/2.3/2.7
3100159	user11c	3	1/18/11 16:40:04	562	RGOM/-60/32/2.1/1.0/3.0/2.6/1.8
3100159	user11c	3	1/18/11 16:40:11	560	RGCP/11/58/2.0/1.0/2.5/2.5/1.9
3100161	user12a	3	1/18/11 17:56:51	1348	DISC/-58/0/2.6/4.0/2.0/4.3/0.0
3100161	user12a	3	1/18/11 17:57:31	1182	RGPD/14/0/3.1/3.4/2.0/4.3/2.5
3100161	user12a	3	1/18/11 17:57:42	1206	RGCF/15/84/3.1/3.5/2.0/4.2/2.9
3100161	user12a	1	1/18/11 17:57:54	1184	RGCP/11/87/3.0/3.4/2.0/4.1/2.4
3100161	user12b	3	1/18/11 17:59:15	1252	RGPD/14/0/3.2/3.7/1.5/4.0/3.5
3100161	user12b	3	1/18/11 17:59:25	1232	RGCP/10/69/2.8/3.6/1.5/4.1/1.9
3100161	user12c	3	1/18/11 18:00:37	866	RGPD/14/0/2.9/2.2/2.0/4.3/3.2
3100161	user12c	3	1/18/11 18:00:46	892	RGCP/10/76/2.5/2.3/2.0/4.3/1.3
3100161	user13a	3	1/19/11 10:39:14	1058	RGPD/14/0/2.9/2.9/1.5/4.0/3.0
3100161	user13a	3	1/19/11 10:39:25	992	RGCP/10/63/2.7/2.7/1.5/3.8/2.7
3100161	user13a	1	1/19/11 10:39:45	958	PASS/12/72/2.8/2.5/1.5/3.9/3.3
3100161	user13a	1	1/20/11 15:10:18	808	DENI/-55/49/1.9/1.9/1.0/1.7/2.9

Pen SN	UserID	Mode	LogDate	DataSize	Result
3100161	user13a	1	1/20/11 15:10:30	934	PASS/1/65/2.5/2.4/2.0/2.1/3.5
3100161	user13b	3	1/19/11 10:40:43	300	DISC/-58/0/1.9/0.0/2.0/2.8/2.7
3100161	user13b	3	1/19/11 10:41:02	626	RGPD/14/0/2.5/1.2/3.5/2.2/2.9
3100161	user13b	3	1/19/11 10:41:50	1016	RGPD/14/0/3.1/2.7/3.5/3.3/2.9
3100161	user13b	3	1/19/11 10:42:06	864	RGCP/10/58/3.0/2.2/3.5/3.2/3.0
3100161	user13b	1	1/20/11 15:11:11	916	DENI/-55/42/2.6/2.4/2.0/2.2/3.8
3100161	user13b	1	1/20/11 15:11:22	944	DENI/-55/30/2.3/2.5/2.0/2.5/2.3
3100161	user13b	1	1/20/11 15:11:32	882	SVBS/444
3100161	user13b	1	1/20/11 15:11:44	574	DENI/-55/0/2.1/1.0/0.0/3.7/3.6
3100161	user14a	3	1/19/11 10:44:15	848	RGPD/14/0/2.5/2.1/1.0/3.8/3.1
3100161	user14a	3	1/19/11 10:44:28	886	RGOM/-60/21/2.4/2.2/0.5/3.5/3.5
3100161	user14a	3	1/19/11 10:44:47	776	RGIC/-55/51/2.2/1.8/0.5/3.7/2.8
3100161	user14a	3	1/19/11 10:45:03	856	RGPD/14/0/2.3/2.1/1.5/3.5/1.9
3100161	user14a	3	1/19/11 10:45:14	828	RGOM/-60/59/2.4/2.0/1.0/3.9/2.8
3100161	user14a	3	1/19/11 10:45:30	790	RGIC/-55/26/2.2/1.9/0.5/3.6/2.9
3100161	user14a	3	1/19/11 10:46:11	880	RGPD/14/0/2.6/2.2/1.5/3.6/3.1
3100161	user14a	3	1/19/11 10:46:21	916	RGCF/15/67/2.5/2.4/1.5/3.3/3.0
3100161	user14a	1	1/19/11 10:46:33	864	RGCP/11/71/2.4/2.2/1.5/3.9/2.2
3100161	user14a	1	1/19/11 10:46:57	932	PASS/11/72/2.8/2.4/1.5/3.9/3.2
3100161	user14b	3	1/19/11 10:48:17	956	RGPD/14/0/3.3/2.5/5.0/2.4/3.1
3100161	user14b	3	1/19/11 10:48:40	1226	RGOM/-60/15/3.1/3.6/5.0/1.9/2.1
3100161	user14b	3	1/19/11 10:48:51	1174	RGCP/12/65/3.6/3.4/5.0/2.5/3.4
3100161	user15a	3	1/19/11 11:04:00	808	DISC/-58/0/1.5/1.9/1.0/9.0/3.2
3100161	user15a	3	1/19/11 11:04:13	696	RGPD/14/0/2.4/1.5/1.0/4.4/2.6
3100161	user15a	3	1/19/11 11:04:22	680	RGCP/10/58/2.3/1.5/1.0/4.5/2.2
3100161	user15b	3	1/19/11 11:05:12	174	DISC/-58/0/1.3/0.0/0.0/4.4/0.9
3100161	user15b	3	1/19/11 11:05:21	340	DISC/-58/0/1.0/0.1/0.0/3.9/0.0
3100161	user15b	3	1/19/11 11:05:31	282	DISC/-58/0/1.5/0.0/0.0/3.9/2.2
3100161	user15b	3	1/19/11 11:05:43	612	DISC/-58/0/1.0/1.2/0.5/9.0/2.3
3100161	user15b	3	1/19/11 11:05:53	572	RGPD/14/0/1.9/1.0/0.5/3.9/2.3
3100161	user15b	3	1/19/11 11:06:02	552	RGCP/10/85/2.1/1.0/0.5/4.1/2.7
3100161	user16a	3	1/19/11 11:09:42	872	RGPD/14/0/2.6/2.2/2.0/3.9/2.2
3100161	user16a	3	1/19/11 11:09:52	834	RGCP/10/75/2.6/2.0/2.0/3.7/2.6
3100161	user16a	1	1/20/11 11:31:04	832	SVBS/444
3100161	user16a	1	1/20/11 11:31:19	936	PASS/11/61/2.7/2.4/2.0/3.8/2.6
3100161	user16b	3	1/19/11 11:10:45	362	RGPD/14/0/1.2/0.2/0.5/2.7/1.5
3100161	user16b	3	1/19/11 11:10:54	866	RGOM/-60/0/3.2/2.2/4.5/3.7/2.2
3100161	user16b	3	1/19/11 11:11:07	818	RGCP/12/61/3.3/2.0/4.5/4.0/2.8
3100161	user16b	1	1/20/11 11:31:47	902	DENI/-55/0/2.5/2.3/4.0/3.7/0.0
3100161	user16b	1	1/20/11 11:31:58	886	DENI/-55/0/2.5/2.2/4.5/3.1/0.0

Pen SN	UserID	Mode	LogDate	DataSize	Result
3100161	user16b	1	1/20/11 11:32:13	810	DENI/-55/57/2.7/2.0/4.0/3.5/1.1
3100161	user16b	1	1/20/11 11:32:43	894	DENI/-55/24/3.0/2.3/3.0/3.6/3.3
3100161	user16b	1	1/20/11 11:33:07	234	DENI/-55/0/0.5/0.0/0.5/1.5/0.0
3100161	user16b	1	1/20/11 11:33:25	930	DENI/-55/0/2.5/2.4/4.5/3.0/0.0
3100161	user16b	1	1/20/11 11:33:42	882	DENI/-55/0/2.3/2.2/4.0/3.0/0.0
3100161	user16b	1	1/20/11 11:33:54	852	DENI/-55/32/2.5/2.1/3.5/3.0/1.3
3100161	user16b	1	1/20/11 11:34:02	720	DENI/-55/34/2.3/1.6/3.0/3.4/1.3
3100161	user16b	1	1/20/11 11:34:14	892	DENI/-55/36/2.7/2.3/3.0/3.7/1.9
3100161	user17a	3	1/19/11 11:27:20	580	RGPD/14/0/2.2/1.1/1.0/3.2/3.5
3100161	user17a	3	1/19/11 11:27:33	650	RGOM/-60/38/1.8/1.3/1.0/2.9/2.1
3100161	user17a	3	1/19/11 11:27:45	594	RGCP/11/64/1.7/1.1/1.5/2.9/1.3
3100161	user17b	3	1/19/11 11:28:37	484	RGPD/14/0/2.0/0.7/2.0/3.4/1.8
3100161	user17b	3	1/19/11 11:28:45	474	RGCP/10/79/2.0/0.7/2.0/3.0/2.5
3100161	user18a	3	1/19/11 11:30:57	1466	RGPD/14/0/3.7/4.5/3.5/3.4/3.4
3100161	user18a	3	1/19/11 11:31:12	1396	RGOM/-60/52/3.5/4.2/3.0/4.0/3.0
3100161	user18a	3	1/19/11 11:31:27	1294	RGCP/12/77/3.4/3.8/3.0/3.5/3.3
3100161	user18b	3	1/19/11 11:32:26	950	RGPD/14/0/2.8/2.5/2.5/3.6/2.7
3100161	user18b	3	1/19/11 11:32:37	792	RGCF/15/69/2.7/1.9/2.5/3.5/3.0
3100161	user18b	1	1/19/11 11:32:48	842	RGIC/-55/47/2.7/2.1/2.0/3.4/3.4
3100161	user18b	3	1/19/11 11:33:11	518	RGPD/14/0/1.9/0.8/0.5/4.1/1.9
3100161	user18b	3	1/19/11 11:33:21	486	RGCP/10/90/1.9/0.7/0.5/4.0/2.5
3100161	user19a	3	1/19/11 11:35:41	1062	RGPD/14/0/2.5/2.9/1.5/2.9/2.6
3100161	user19a	3	1/19/11 11:35:51	1012	RGOM/-60/51/2.8/2.7/2.5/2.6/3.5
3100161	user19a	3	1/19/11 11:36:03	998	RGCP/11/67/2.7/2.7/1.5/3.1/3.4
3100161	user19a	1	1/19/11 11:36:31	968	PASS/12/74/2.4/2.6/2.0/2.1/2.8
3100161	user19a	1	1/19/11 11:46:34	1018	PASS/1/72/3.0/2.8/1.5/4.1/3.5
3100156	user19a	1	1/19/11 11:50:44	1066	DENI/-55/0/1.6/2.9/1.5/9.0/1.9
3100156	user19a	1	1/19/11 11:51:03	1040	PASS/1/67/3.0/2.8/1.5/4.5/3.3
3100161	user19b	3	1/19/11 11:37:55	998	RGPD/14/0/3.4/2.7/5.0/2.3/3.5
3100161	user19b	3	1/19/11 11:38:17	988	RGCP/10/50/3.1/2.6/5.0/1.6/3.2
3100164	user20a	3	1/19/11 11:52:56	568	RGPD/14/0/2.1/1.0/1.0/4.0/2.4
3100164	user20a	3	1/19/11 11:53:03	284	RGOM/-60/0/1.8/0.0/0.5/4.2/2.7
3100164	user20a	3	1/19/11 11:53:09	280	RGIC/-55/0/1.7/0.0/0.5/4.0/2.2
3100164	user20a	3	1/19/11 11:53:36	488	RGPD/14/0/2.0/0.7/1.0/3.9/2.5
3100164	user20a	3	1/19/11 11:53:44	470	RGCP/10/59/2.2/0.6/1.0/3.9/3.3
3100164	user20b	3	1/19/11 11:55:01	24	DISC/-58/0/1.1/0.0/0.0/3.9/0.6
3100164	user20b	3	1/19/11 11:56:23	76	DISC/-58/0/1.2/0.0/0.5/4.2/9.0
3100161	user21a	3	1/19/11 14:15:06	442	RGPD/14/0/2.2/0.5/1.5/3.8/3.0
3100161	user21a	3	1/19/11 14:15:15	464	RGCP/10/53/2.4/0.6/1.5/4.2/3.2
3100161	user21a	1	1/20/11 11:23:08	436	PASS/11/73/2.2/0.5/1.5/3.0/3.8

Pen SN	UserID	Mode	LogDate	DataSize	Result
3100161	user21b	3	1/19/11 14:16:16	440	RGPD/14/0/1.7/0.5/1.0/2.7/2.5
3100161	user21b	3	1/19/11 14:16:32	1034	RGPD/14/0/3.2/2.8/5.0/1.8/3.1
3100161	user21b	3	1/19/11 14:16:43	1138	RGOM/-60/17/3.2/3.2/5.0/1.7/2.8
3100161	user21b	3	1/19/11 14:17:00	1296	RGIC/-55/29/3.4/3.8/5.0/1.9/2.9
3100161	user21b	3	1/19/11 14:17:09	76	DISC/-58/0/0.5/0.0/0.5/1.5/0.0
3100161	user21b	3	1/19/11 14:17:20	888	RGPD/14/0/3.1/2.3/5.0/1.8/3.3
3100161	user21b	3	1/19/11 14:17:29	1050	RGOM/-60/32/3.3/2.9/5.0/2.1/3.3
3100161	user21b	3	1/19/11 14:17:39	992	RGIC/-55/33/3.0/2.7/4.5/1.9/2.9
3100161	user21b	3	1/19/11 14:18:06	1026	RGPD/14/0/3.5/2.8/5.0/2.8/3.5
3100161	user21b	3	1/19/11 14:18:15	1086	RGCF/15/72/3.5/3.0/5.0/2.5/3.4
3100161	user21b	1	1/19/11 14:18:26	1078	RGIC/-55/53/3.5/3.0/5.0/2.7/3.2
3100161	user21b	3	1/19/11 14:18:47	526	RGPD/14/0/2.2/0.9/2.5/2.3/3.1
3100161	user21b	3	1/19/11 14:18:58	660	RGCP/10/51/2.3/1.4/2.5/2.7/2.6
3100161	user21b	1	1/20/11 11:23:53	740	DENI/-55/33/2.2/1.7/3.0/1.4/2.7
3100161	user21b	1	1/20/11 11:24:07	940	DENI/-55/0/2.0/2.5/3.0/2.5/0.0
3100161	user21b	1	1/20/11 11:24:23	340	DENI/-55/0/0.8/0.1/0.5/1.7/1.0
3100161	user21b	1	1/20/11 11:24:31	698	DENI/-55/47/2.1/1.5/2.5/2.2/2.2
3100161	user21b	1	1/20/11 11:24:40	716	DENI/-55/21/2.1/1.6/3.0/2.2/1.7
3100161	user21b	1	1/20/11 11:25:00	670	DENI/-55/41/2.1/1.4/3.0/2.5/1.7
3100161	user21b	1	1/20/11 11:27:53	590	PASS/11/53/2.2/1.1/2.5/1.7/3.5
3100161	user22a	3	1/19/11 16:07:47	602	RGPD/14/0/2.7/1.2/4.0/1.9/3.8
3100164	user22a	3	1/19/11 16:15:53	900	RGPD/14/0/3.1/2.3/3.0/3.1/3.8
3100164	user22a	3	1/19/11 16:16:02	950	RGCP/10/57/3.0/2.5/3.0/3.9/2.7
3100164	user22b	3	1/19/11 16:17:09	994	RGPD/14/0/3.1/2.7/2.0/3.2/4.3
3100164	user22b	3	1/19/11 16:17:19	1026	RGOM/-60/20/3.2/2.8/2.5/3.8/3.8
3100164	user22b	3	1/19/11 16:17:28	966	RGCP/12/71/3.2/2.6/2.5/4.2/3.4
3100164	user22b	1	1/19/11 16:17:49	892	FLAG/4/57/2.9/2.3/2.0/3.2/4.0
3100164	user22b	1	1/19/11 16:17:58	868	PASS/12/72/2.9/2.2/2.5/3.6/3.5
3100164	user23a	3	1/19/11 16:24:41	820	RGPD/14/0/2.8/2.0/1.0/3.7/4.4
3100164	user23a	3	1/19/11 16:24:51	732	RGCP/10/56/2.5/1.7/1.0/3.1/4.1
3100164	user23a	1	1/19/11 16:25:13	688	PASS/12/76/2.2/1.5/1.0/3.0/3.3
3100164	user23b	3	1/19/11 16:25:50	1332	RGPD/14/0/3.5/4.0/3.0/2.8/4.3
3100164	user23b	3	1/19/11 16:26:01	1592	RGOM/-60/46/3.8/5.0/2.5/3.4/4.3
3100164	user23b	3	1/19/11 16:26:12	1530	RGCP/12/68/3.7/4.7/2.5/3.3/4.3
3100161	user24a	3	1/19/11 17:03:02	1062	RGPD/14/0/2.8/2.9/2.5/2.5/3.5
3100161	user24a	3	1/19/11 17:03:13	958	RGOM/-60/58/2.8/2.5/2.0/3.0/3.9
3100161	user24a	3	1/19/11 17:03:26	1016	RGIC/-55/0/2.0/2.7/2.5/2.6/0.0
3100161	user24a	3	1/19/11 17:03:54	1162	DISC/-58/0/2.0/3.3/2.0/2.8/0.0
3100161	user24a	3	1/19/11 17:04:20	1124	RGPD/14/0/2.3/3.2/2.0/2.2/1.7
3100161	user24a	3	1/19/11 17:04:32	1126	RGCP/10/78/2.1/3.2/1.5/2.2/1.7

Pen SN	UserID	Mode	LogDate	DataSize	Result
3100161	user24a	1	1/19/11 17:04:49	1098	PASS/11/75/2.4/3.1/2.0/2.6/1.9
3100161	user24a	1	1/19/11 17:09:22	982	PASS/1/72/2.6/2.6/2.0/3.1/2.6
3100161	user24a	1	1/19/11 17:10:27	1412	DENI/-55/72/3.2/4.3/2.0/3.2/3.2
3100161	user24b	3	1/19/11 17:06:57	1362	RGPD/14/0/3.6/4.1/4.0/2.9/3.4
3100161	user24b	3	1/19/11 17:07:10	1346	RGOM/-60/8/3.6/4.0/5.0/2.5/3.1
3100161	user24b	3	1/19/11 17:07:27	1194	RGIC/-55/33/2.9/3.4/3.5/3.1/1.8
3100161	user24b	3	1/19/11 17:08:09	1504	RGPD/14/0/3.4/4.6/4.0/3.0/2.1
3100161	user24b	3	1/19/11 17:08:21	1550	RGOM/-60/43/3.9/4.8/5.0/2.8/2.8
3100161	user24b	3	1/19/11 17:08:34	1500	RGCP/11/57/3.8/4.6/5.0/3.1/2.5
3100161	user25a	3	1/19/11 17:18:29	550	RGPD/14/0/2.1/1.0/2.0/3.2/2.1
3100161	user25a	3	1/19/11 17:18:39	574	RGCP/10/74/2.6/1.0/2.0/4.3/3.2
3100161	user25a	1	1/19/11 17:19:16	514	PASS/11/83/2.2/0.8/2.0/3.9/1.9
3100161	user25a	1	1/19/11 17:19:41	540	DENI/-55/6/2.0/0.9/1.0/2.5/3.6
3100159	user30a	3	1/20/11 11:00:16	1112	RGPD/14/0/3.3/3.1/4.5/3.2/2.4
3100159	user30a	3	1/20/11 11:00:55	1160	RGOM/-60/39/3.4/3.3/4.0/3.6/2.6
3100159	user30a	3	1/20/11 11:01:11	1124	RGIC/-55/43/3.6/3.2/5.0/3.9/2.4
3100159	user30a	3	1/20/11 11:02:49	1302	RGPD/14/0/3.9/3.8/4.5/4.1/3.0
3100159	user30a	3	1/20/11 11:03:07	1314	RGOM/-60/33/3.9/3.9/4.0/4.2/3.4
3100159	user30a	3	1/20/11 11:03:21	1232	RGCP/12/72/3.8/3.6/4.0/4.4/3.1
3100161	user30a	1	1/20/11 16:11:23	1040	PASS/12/54/3.3/2.8/4.0/2.7/3.5
3100161	user30a	1	1/20/11 16:11:59	1348	DENI/-55/25/3.8/4.0/5.0/2.7/3.6
3100161	user30a	1	1/20/11 16:12:13	32	DENI/-55/0/0.6/0.0/0.0/0.6/1.8
3100161	user30a	1	1/20/11 16:12:23	1114	DENI/-55/23/3.2/3.1/3.5/2.8/3.3
3100161	user30a	1	1/20/11 16:12:37	1256	DENI/-55/39/3.7/3.7/5.0/2.3/4.0
3100161	user30a	1	1/20/11 16:12:52	1124	DENI/-55/33/3.1/3.2/4.0/2.4/3.0
3100161	user30a	1	1/20/11 16:13:11	1108	DENI/-55/15/3.6/3.1/5.0/2.4/3.7
3100161	user30a	1	1/20/11 16:13:31	1172	DENI/-55/27/3.6/3.3/4.5/2.8/3.7
3100161	user30a	1	1/20/11 16:14:00	1004	DENI/-55/18/2.8/2.7/3.5/2.2/2.9
3100161	user30a	1	1/20/11 16:15:10	1044	DENI/-55/27/3.0/2.9/3.0/2.4/3.6
3100161	user30a	1	1/20/11 16:15:33	1158	DENI/-55/45/3.3/3.3/4.0/2.0/3.9
3100161	user31a	3	1/20/11 11:42:50	576	RGPD/14/0/2.2/1.1/1.5/4.1/2.3
3100161	user31a	3	1/20/11 11:42:59	614	RGCP/10/82/2.2/1.2/1.5/4.2/1.9
3100161	user31a	1	1/20/11 11:43:35	620	PASS/12/82/2.3/1.2/1.5/3.8/2.7
3100161	user31a	1	1/20/11 11:43:59	588	DENI/-55/51/2.2/1.1/1.5/4.0/2.3
3100161	user31a	1	1/20/11 11:44:10	676	DENI/-55/57/2.6/1.4/1.5/3.7/3.8
3100161	user31a	1	1/20/11 11:44:18	666	DENI/-55/52/2.4/1.4/1.5/3.6/3.0
3100161	user31a	1	1/20/11 11:44:33	636	FLAG/4/65/2.7/1.3/2.0/3.8/3.9
3100161	user31a	1	1/20/11 11:44:46	598	PASS/1/81/2.4/1.1/1.5/3.6/3.2
3100161	user31a	1	1/21/11 16:08:00	564	DENI/-55/49/1.9/1.0/1.5/2.2/2.8
3100161	user31a	1	1/21/11 16:08:08	556	PASS/1/81/2.1/1.0/1.5/2.5/3.4

Pen SN	UserID	Mode	LogDate	DataSize	Result
3100161	user32a	3	1/20/11 11:50:34	614	RGPD/14/0/1.9/1.2/2.0/1.8/2.5
3100161	user32a	3	1/20/11 11:50:43	628	RGCP/10/66/2.0/1.3/2.0/1.6/3.0
3100161	user32a	1	1/20/11 16:19:51	554	PASS/12/66/1.9/1.0/2.0/1.2/3.4
3100161	user32a	1	1/20/11 16:20:30	578	PASS/1/68/1.8/1.1/2.0/1.3/3.0
3100161	user33a	3	1/20/11 12:32:41	552	RGPD/14/0/2.5/1.0/3.5/2.1/3.5
3100161	user33a	3	1/20/11 12:33:13	582	RGOM/-60/38/2.7/1.1/3.5/2.8/3.5
3100161	user33a	3	1/20/11 12:33:24	544	RGCP/12/58/2.8/0.9/3.5/3.3/3.4
3100161	user33a	1	1/20/11 12:34:23	542	DENI/-55/40/2.9/0.9/3.5/3.4/3.8
3100161	user33a	1	1/20/11 12:34:39	498	DENI/-55/39/2.7/0.8/3.5/3.1/3.5
3100161	user33a	1	1/20/11 12:34:53	514	PASS/12/57/2.8/0.8/3.5/3.8/3.2
3100161	user34a	3	1/20/11 12:41:12	956	RGPD/14/0/3.1/2.5/2.0/4.3/3.7
3100161	user34a	3	1/20/11 12:41:22	1090	RGOM/-60/12/3.3/3.0/2.0/4.6/3.7
3100161	user34a	3	1/20/11 12:41:32	1036	RGCP/11/70/3.2/2.8/2.0/4.4/3.7
3100161	user35a	3	1/20/11 12:54:34	766	RGPD/14/0/2.2/1.8/1.0/3.1/3.0
3100161	user35a	3	1/20/11 12:54:43	870	RGOM/-60/41/2.1/2.2/1.0/2.5/2.9
3100161	user35a	3	1/20/11 12:55:14	828	RGIC/-55/48/2.3/2.0/1.0/3.1/3.3
3100161	user35a	3	1/20/11 12:56:02	830	RGPD/14/0/2.4/2.0/1.5/2.4/3.6
3100161	user35a	3	1/20/11 12:56:12	758	RGOM/-60/54/2.3/1.8/1.0/2.5/4.0
3100161	user35a	3	1/20/11 12:56:21	778	RGCP/12/83/2.4/1.8/1.0/2.8/4.0
3100161	user35a	1	1/20/11 12:58:00	744	FLAG/4/62/2.3/1.7/1.0/2.8/3.7
3100161	user35a	1	1/20/11 12:58:15	778	PASS/4/64/2.6/1.8/1.5/3.3/3.7
3100161	user35a	1	1/20/11 12:58:39	632	DENI/-55/45/2.3/1.3/1.5/3.3/3.1
3100161	user35a	1	1/20/11 12:59:31	534	DENI/-55/0/1.8/0.9/0.5/2.6/3.0
3100161	user35a	1	1/20/11 13:00:09	746	DENI/-55/61/2.4/1.7/1.5/2.6/3.6
3100161	user35a	1	1/20/11 13:00:36	718	FLAG/4/57/2.2/1.6/1.0/3.3/2.9
3100161	user35a	1	1/20/11 13:01:22	750	DENI/-55/54/2.3/1.7/1.5/2.7/3.3
3100161	user35a	1	1/20/11 13:01:33	766	DENI/-55/49/2.0/1.8/1.0/2.5/2.8
3100161	user35a	1	1/20/11 13:01:43	816	DENI/-55/60/2.5/2.0/1.5/2.8/3.7
3100161	user35a	1	1/20/11 13:02:01	868	DENI/-55/49/2.5/2.2/1.5/3.4/3.0
3100161	user35a	1	1/20/11 13:02:19	754	DENI/-55/50/2.3/1.7/1.5/2.8/3.1
3100161	user35a	1	1/20/11 13:02:28	802	DENI/-55/55/2.3/1.9/1.5/2.8/3.0
3100161	user35a	1	1/20/11 13:02:43	332	DENI/-55/0/1.6/0.1/0.5/3.0/2.6
3100161	user35a	1	1/20/11 13:02:55	658	DENI/-55/59/1.8/1.4/0.5/3.2/2.0
3100161	user35a	1	1/20/11 13:03:16	612	DENI/-55/53/2.0/1.2/0.5/3.2/3.0
3100159	user35a	1	1/20/11 13:03:48	730	DENI/-55/62/2.1/1.6/0.5/3.7/2.5
3100159	user35a	1	1/20/11 13:04:07	846	DENI/-55/49/2.8/2.1/1.5/4.5/3.2
3100161	user35a	1	1/20/11 13:14:19	774	DENI/-55/49/2.2/1.8/1.5/2.7/2.8
3100161	user35a	1	1/20/11 13:14:45	826	DENI/-55/45/2.2/2.0/1.5/2.7/2.6
3100161	user35b	3	1/20/11 13:16:15	568	RGPD/14/0/2.5/1.0/3.5/2.7/2.6
3100161	user35b	3	1/20/11 13:16:26	582	RGOM/-60/24/2.6/1.1/2.5/3.3/3.5

Pen SN	UserID	Mode	LogDate	DataSize	Result
3100161	user35b	3	1/20/11 13:16:46	576	RGCP/12/75/2.4/1.1/2.5/3.2/2.9
3100161	user35b	1	1/20/11 13:17:07	518	DENI/-55/43/2.6/0.8/2.5/3.3/3.5
3100161	user35b	1	1/20/11 13:17:18	560	FLAG/4/48/2.1/1.0/2.5/2.7/2.1
3100161	user35b	1	1/20/11 13:17:33	588	DENI/-55/50/2.4/1.1/2.5/2.8/3.2
3100161	user35b	1	1/20/11 13:17:43	552	PASS/11/65/2.7/1.0/2.5/3.4/4.0
3100161	user36a	3	1/20/11 16:25:56	1466	RGPD/14/0/3.7/4.5/3.0/3.9/3.5
3100161	user36a	3	1/20/11 16:26:32	1488	RGCP/10/77/3.8/4.6/3.0/3.7/3.7
3100161	user36a	1	1/20/11 16:27:05	1446	PASS/12/74/3.7/4.4/3.0/3.5/3.8
3100161	user36a	1	1/20/11 16:27:21	1432	DENI/-55/36/3.0/4.3/2.5/3.0/2.3
3100161	user36a	1	1/20/11 16:27:46	1418	DENI/-55/55/3.5/4.3/2.5/3.8/3.6
3100161	user37a	3	1/20/11 17:05:33	1208	RGPD/14/0/3.1/3.5/4.0/2.4/2.5
3100161	user37a	3	1/20/11 17:06:03	1294	RGOM/-60/36/3.4/3.8/4.5/2.7/2.5
3100161	user37a	3	1/20/11 17:06:16	1334	RGCP/11/57/3.4/4.0/4.0/3.5/2.0
3100161	user37a	1	1/20/11 17:07:01	1370	DENI/-55/17/3.2/4.1/4.0/1.8/2.8
3100161	user37a	1	1/20/11 17:07:16	1528	FLAG/4/49/4.0/4.7/5.0/3.1/3.3
3100161	user37a	1	1/20/11 17:07:35	1482	PASS/12/53/3.4/4.5/4.0/3.0/2.0
3100161	user40a	3	1/21/11 10:34:35	292	DISC/-58/0/1.5/0.0/1.0/4.8/0.0
3100161	user40a	3	1/21/11 10:35:06	790	RGPD/14/0/3.1/1.9/3.0/4.2/3.4
3100161	user40a	3	1/21/11 10:35:17	832	RGOM/-60/42/3.0/2.0/3.0/4.5/2.4
3100161	user40a	3	1/21/11 10:35:30	732	RGIC/-55/54/2.8/1.7/2.5/4.3/2.6
3100161	user40a	3	1/21/11 10:35:59	1310	RGPD/14/0/4.2/3.9/5.0/4.1/3.7
3100161	user40a	3	1/21/11 10:36:13	1320	RGOM/-60/40/4.2/3.9/5.0/4.2/3.9
3100161	user40a	3	1/21/11 10:36:27	1290	RGIC/-55/39/4.2/3.8/5.0/4.3/3.8
3100161	user40a	3	1/21/11 10:37:08	1478	RGPD/14/0/4.3/4.5/5.0/4.2/3.6
3100161	user40a	3	1/21/11 10:37:19	1408	RGOM/-60/26/4.2/4.3/5.0/4.1/3.4
3100161	user40a	3	1/21/11 10:37:31	1336	RGCP/12/62/3.9/4.0/4.0/4.1/3.3
3100161	userx	3	1/20/11 17:24:19	544	RGPD/14/0/1.7/0.9/0.5/3.4/1.9
3100161	userx	3	1/20/11 17:24:38	948	RGPD/14/0/2.9/2.5/2.5/4.9/1.7
3100161	userx	3	1/20/11 17:24:49	924	RGCP/10/80/2.6/2.4/2.5/4.3/1.1
3100161	userx	1	1/20/11 17:25:11	786	DENI/-55/0/2.0/1.9/3.0/3.3/0.0
3100161	userx	1	1/20/11 17:25:23	978	DENI/-55/33/3.1/2.6/2.5/4.3/3.1
3100161	userx	1	1/20/11 17:25:32	628	DENI/-55/0/2.7/1.3/2.0/4.0/3.6
3100161	userx	1	1/20/11 17:25:48	906	DENI/-55/0/2.1/2.3/2.5/3.5/0.0
3100161	userx	1	1/20/11 17:26:00	894	PASS/12/86/2.6/2.3/2.5/4.0/1.5
3100161	userx	1	1/20/11 17:26:50	746	PASS/1/75/2.7/1.7/2.5/3.7/2.8
3100161	userx	1	1/20/11 17:27:18	738	PASS/1/77/2.8/1.7/2.5/3.5/3.7
3100161	userx	1	1/20/11 17:27:28	738	DENI/-55/15/2.0/1.7/2.5/1.4/2.5
3100161	userx	1	1/20/11 17:27:43	524	DENI/-55/0/1.6/0.9/2.0/1.1/2.7
3100161	userx	1	1/20/11 17:27:59	590	DENI/-55/0/1.6/1.1/2.5/2.6/0.0
3100161	userx	1	1/20/11 17:28:08	686	PASS/1/69/2.3/1.5/2.5/2.9/2.3

Pen SN	UserID	Mode	LogDate	DataSize	Result
3100161	userx	1	1/20/11 17:28:19	570	DENI/-55/0/1.7/1.0/2.5/1.0/2.2
3100161	userx	1	1/20/11 17:28:41	646	DENI/-55/0/2.1/1.3/2.5/2.3/2.1
3100161	userx	1	1/20/11 17:28:50	730	PASS/1/69/2.5/1.6/2.5/2.7/3.1
3100161	userx	1	1/20/11 17:29:04	460	DENI/-55/0/2.1/0.6/2.0/3.2/2.5
3100161	userx	1	1/20/11 17:29:16	588	DENI/-55/0/1.7/1.1/2.5/1.4/2.0
3100161	userx	1	1/20/11 17:29:27	568	DENI/-55/0/1.8/1.0/2.5/1.5/2.1
3100161	userx	1	1/20/11 17:29:36	590	DENI/-55/0/1.9/1.1/2.5/1.7/2.2
3100161	userx	1	1/20/11 17:30:10	690	DENI/-55/28/1.9/1.5/3.0/1.6/1.6
3100161	userx	1	1/20/11 17:30:17	672	DENI/-55/40/2.0/1.4/2.5/1.9/2.0
3100161	userx	1	1/20/11 17:30:39	608	DENI/-55/0/1.8/1.2/2.5/2.2/1.3
3100161	userx	1	1/20/11 17:30:48	678	SVBS/444
3100161	userx	1	1/20/11 17:30:58	664	FLAG/4/63/2.5/1.4/2.5/2.5/3.5
3100161	userx	1	1/20/11 17:31:08	732	PASS/1/64/1.9/1.7/2.5/2.1/1.5
3100161	userx	1	1/20/11 17:31:25	730	DENI/-55/41/2.3/1.6/2.5/2.4/2.9
3100161	userx	1	1/20/11 17:31:43	748	DENI/-55/39/2.0/1.7/2.5/1.9/2.0
3100161	userx	1	1/20/11 17:31:54	772	DENI/-55/40/2.6/1.8/2.5/3.0/3.0
3100161	userx	1	1/20/11 17:32:09	1178	DENI/-55/8/2.9/3.4/3.0/2.3/2.9
3100161	userx	1	1/20/11 17:32:38	624	DENI/-55/0/1.7/1.2/2.0/1.9/1.9
3100161	userx	1	1/20/11 17:32:46	538	DENI/-55/0/1.9/0.9/2.5/2.0/2.1
3100161	userx	1	1/20/11 17:33:01	554	DENI/-55/0/1.9/1.0/2.5/2.2/1.9
3100161	userx	1	1/20/11 17:33:09	628	DENI/-55/0/1.5/1.3/2.5/2.1/0.0
3100161	userx	1	1/20/11 17:33:18	534	DENI/-55/0/1.8/0.9/2.5/2.3/1.5
3100161	userx	1	1/20/11 17:33:27	532	DENI/-55/0/1.9/0.9/2.5/1.8/2.6
3100161	userx	1	1/20/11 17:40:59	698	PASS/1/73/2.0/1.5/2.5/2.2/1.6
3100161	userx	1	1/20/11 17:41:58	756	FLAG/4/54/2.1/1.7/2.5/1.8/2.3
3100161	userx	1	1/20/11 17:42:10	628	DENI/-55/0/1.4/1.3/2.5/1.8/0.0
3100161	userx	1	1/20/11 17:42:22	602	DENI/-55/0/1.7/1.2/2.5/2.1/1.1
3100161	userx	1	1/20/11 17:42:32	722	SVBS/444
3100161	userx	1	1/20/11 17:42:44	686	SVBS/444
3100161	userx	1	1/20/11 17:42:57	726	DENI/-55/59/1.9/1.6/2.5/2.1/1.2
3100161	userx	1	1/20/11 17:43:08	814	DENI/-55/41/2.3/2.0/2.5/2.4/2.5
3100161	userx	1	1/20/11 17:43:19	820	PASS/1/77/2.2/2.0/2.5/2.3/1.9
3100161	userx	1	1/20/11 17:43:38	818	PASS/1/76/2.0/2.0/2.5/2.3/1.2
3100161	userx	1	1/20/11 17:43:51	844	PASS/1/64/2.5/2.1/2.5/2.2/3.1
3100161	userx	1	1/21/11 10:41:32	680	PASS/4/61/2.8/1.5/2.5/3.5/3.7
3100161	userx	1	1/21/11 10:42:05	500	DENI/-55/0/2.4/0.8/2.0/3.8/3.1
3100161	userx	1	1/21/11 10:42:34	666	DENI/-55/43/2.5/1.4/2.5/3.2/2.7
3100161	userx	1	1/21/11 16:11:46	662	DENI/-55/0/1.6/1.4/2.5/2.6/0.0
3100161	userx	1	1/21/11 16:11:54	692	PASS/1/65/2.4/1.5/2.5/3.5/2.0
3100161	userx	1	1/21/11 16:12:22	548	DENI/-55/0/1.0/0.9/1.0/2.3/0.0

Pen SN	UserID	Mode	LogDate	DataSize	Result
3100161	userx	1	1/21/11 16:12:32	440	DENI/-55/0/0.7/0.5/0.5/1.7/0.0
3100161	userx	1	1/21/11 16:12:45	852	DENI/-55/0/1.6/2.1/2.5/1.8/0.0
3100161	userx	1	1/21/11 16:13:22	946	DENI/-55/49/2.3/2.5/1.5/4.1/1.2
3100161	userx	1	1/21/11 16:13:30	68	DENI/-55/0/1.2/0.0/0.5/3.1/1.2
3100161	userx	1	1/21/11 16:25:04	412	DENI/-55/0/1.0/0.4/1.0/1.5/1.0
3100161	userx	1	1/21/11 16:25:14	708	DENI/-55/59/2.0/1.6/3.0/1.6/1.8
3100161	userx	1	1/21/11 16:25:24	852	PASS/1/75/2.2/2.1/2.5/2.8/1.4
3100161	userx	1	1/21/11 16:26:50	558	DENI/-55/0/1.9/1.0/2.5/2.1/2.2
3100161	userx	1	1/21/11 16:27:05	522	DENI/-55/0/1.5/0.8/1.5/1.9/1.7
3100161	userx	1	1/21/11 16:27:29	736	DENI/-55/2/2.8/1.7/3.0/2.9/3.7
3100161	userx	1	1/21/11 16:28:46	650	DENI/-55/0/1.1/1.3/3.0/0.0/0.0
3100161	userx	1	1/21/11 16:28:57	628	DENI/-55/0/1.9/1.3/3.0/1.0/2.2
3100161	userx	1	1/21/11 16:29:09	600	DENI/-55/0/1.7/1.1/3.0/1.0/1.8
3100161	userx	1	1/21/11 16:29:21	660	DENI/-55/47/2.0/1.4/2.5/1.4/2.6
3100161	userx	1	1/21/11 16:29:30	728	PASS/1/72/2.5/1.6/2.5/3.0/2.7
3100161	userx	1	1/21/11 16:29:59	358	DENI/-55/0/1.6/0.2/2.0/0.9/3.4
3100161	userx	1	1/21/11 16:30:07	406	DENI/-55/0/1.8/0.4/2.5/1.3/2.8
3100161	userx	1	1/22/11 12:35:48	712	DENI/-55/0/1.6/1.6/2.5/2.1/0.0
3100161	userx	1	1/22/11 12:35:55	734	PASS/1/66/1.8/1.7/2.5/1.8/1.1
3100161	userx	1	1/22/11 12:36:10	904	PASS/1/75/2.7/2.3/2.5/2.4/3.7
3100161	redteam1	3	1/21/11 10:18:23	1584	RGPD/14/0/3.7/4.9/2.5/4.1/3.3
3100161	redteam1	3	1/21/11 10:19:07	1666	RGCP/10/75/3.7/5.0/2.5/3.9/3.3
3100161	redteam2	3	1/21/11 10:24:13	1312	RGPD/14/0/3.0/3.9/1.5/3.6/2.8
3100161	redteam2	3	1/21/11 10:24:27	966	RGOM/-60/13/2.5/2.6/0.5/4.2/2.8
3100161	redteam2	3	1/21/11 10:24:50	1132	RGIC/-55/17/3.1/3.2/1.5/4.3/3.4
3100161	redteam2	3	1/21/11 10:26:16	1284	RGPD/14/0/3.2/3.8/2.0/4.5/2.8
3100161	redteam2	3	1/21/11 10:26:26	1096	RGCF/15/59/3.0/3.1/2.0/4.3/2.8
3100161	redteam2	1	1/21/11 10:27:00	1224	RGCP/12/65/3.4/3.5/2.0/4.1/3.7
3100161	redteam3	3	1/21/11 10:30:03	1170	RGPD/14/0/3.0/3.3/1.5/3.9/3.4
3100161	redteam3	3	1/21/11 10:30:13	1066	RGCP/10/64/3.0/2.9/1.5/4.3/3.4
3100161	redteam3	1	1/21/11 16:42:29	132	DENI/-55/0/1.3/0.0/1.0/2.4/1.9
3100161	redteam3	1	1/21/11 16:44:53	1020	PASS/12/64/2.9/2.8/1.5/4.2/3.2
3100161	redteam4	3	1/21/11 10:32:28	456	RGPD/14/0/2.8/0.6/2.0/4.8/3.8
3100161	redteam4	3	1/21/11 10:32:36	458	RGCP/10/58/2.7/0.6/2.0/4.7/3.5
3100161	billybob	3	1/20/11 14:59:46	1102	RGPD/14/0/2.9/3.1/2.0/3.3/3.4
3100161	billybob	3	1/20/11 14:59:57	1238	RGCP/10/72/3.2/3.6/2.0/3.5/3.7
3100161	billybob	1	1/20/11 15:01:28	430	DENI/-55/0/1.3/0.5/0.5/2.1/1.9
3100161	billybob	1	1/20/11 15:06:42	1188	PASS/11/85/2.9/3.4/2.0/3.1/3.2
3100161	billybob	1	1/20/11 15:06:57	1366	PASS/1/81/3.1/4.1/2.0/2.5/3.8
3100161	billybob	1	1/20/11 15:08:02	1286	PASS/1/70/3.1/3.8/2.5/3.0/3.2

Pen SN	UserID	Mode	LogDate	DataSize	Result
3100161	billybob	1	1/20/11 15:08:35	402	DENI/-55/0/1.0/0.4/0.0/1.5/2.0
3100161	billybob	1	1/20/11 15:08:44	38	DENI/-55/0/0.3/0.0/0.0/0.7/0.6
3100161	billybob	1	1/20/11 15:09:14	1140	PASS/1/79/2.8/3.2/2.0/2.8/3.1
3100161	billybob	1	1/20/11 15:12:01	1178	PASS/1/76/3.0/3.4/2.0/2.8/4.0
3100164	billybob	1	1/20/11 16:18:35	722	DENI/-55/0/1.9/1.6/0.5/3.0/2.3
3100164	billybob	1	1/20/11 16:18:47	1332	PASS/1/74/3.1/4.0/2.0/3.4/3.0
3100161	billybob	1	1/20/11 16:21:29	1144	DENI/-55/65/2.8/3.2/2.5/1.9/3.5
3100161	billybob	1	1/20/11 16:21:42	1172	PASS/1/69/2.7/3.3/2.0/2.0/3.4
3100161	billybob	1	1/20/11 16:22:20	1064	DENI/-55/26/2.3/2.9/2.0/1.9/2.3
3100161	billybob	1	1/20/11 16:49:44	826	DENI/-55/39/2.6/2.0/1.0/3.8/3.7
3100161	billybob	1	1/20/11 16:49:55	1274	PASS/1/85/3.1/3.7/2.0/3.6/3.0
3100161	billybob	1	1/20/11 16:51:06	1232	PASS/1/82/2.8/3.6/2.0/2.5/3.3
3100161	billybob	1	1/20/11 16:53:30	1310	PASS/1/68/3.1/3.9/2.5/2.3/3.6
3100161	billybob	1	1/20/11 16:55:02	1170	DENI/-55/56/2.7/3.3/2.5/1.7/3.2
3100161	billybob	1	1/20/11 16:55:17	1400	DENI/-55/8/3.4/4.2/3.0/2.4/3.8
3100161	billybob	1	1/20/11 16:55:31	1612	DENI/-55/0/3.9/5.0/5.0/2.1/3.6
3100161	billybob	1	1/20/11 16:55:43	1304	DENI/-55/11/3.5/3.9/4.5/1.9/3.6
3100161	billybob	1	1/20/11 16:55:56	1188	DENI/-55/58/2.9/3.4/2.5/1.9/3.8
3100161	billybob	1	1/20/11 16:56:10	1260	DENI/-55/33/2.7/3.7/2.5/1.9/2.9
3100161	billybob	1	1/20/11 16:56:38	1372	PASS/1/72/2.8/4.1/2.5/2.2/2.5
3100161	billybob	1	1/20/11 16:57:14	1288	DENI/-55/2/2.9/3.8/3.5/2.0/2.4
3100161	billybob	1	1/20/11 16:57:27	1620	DENI/-55/0/3.2/5.0/2.5/2.5/2.8
3100161	billybob	1	1/20/11 16:57:38	1288	DENI/-55/0/1.9/3.8/1.5/2.1/0.0
3100161	billybob	1	1/20/11 16:58:10	1242	DENI/-55/54/2.9/3.6/2.5/2.2/3.4
3100161	billybob	1	1/20/11 16:58:21	1002	SVBS/444
3100161	billybob	1	1/20/11 16:58:31	358	DENI/-55/0/2.1/0.2/0.5/3.4/4.3
3100161	billybob	1	1/20/11 16:58:50	1358	SVBS/444
3100161	billybob	1	1/20/11 16:59:08	1342	DENI/-55/47/2.9/4.0/3.0/1.9/2.9
3100161	billybob	1	1/20/11 16:59:20	1286	PASS/1/68/2.7/3.8/2.5/1.8/2.7
3100161	billybob	1	1/20/11 17:00:20	36	DENI/-55/0/0.1/0.0/0.0/0.5/0.0
3100161	billybob	1	1/20/11 17:01:28	592	DENI/-55/0/1.5/1.1/0.5/2.0/2.3
3100161	billybob	1	1/21/11 16:06:47	1260	PASS/1/76/2.8/3.7/2.0/2.5/3.1
3100161	billybob	1	1/22/11 12:34:37	1296	DENI/-55/49/2.7/3.8/2.0/2.1/2.8
3100161	billybob	1	1/22/11 12:34:47	1522	DENI/-55/55/3.3/4.7/2.5/2.6/3.3
3100161	billybob	1	1/22/11 12:34:57	1390	PASS/1/77/2.9/4.2/2.0/2.4/3.2
3100161	billybob	1	1/22/11 12:35:36	1398	DENI/-55/38/2.8/4.2/2.0/1.8/3.1

APPENDIX B. INSTITUTIONAL REVIEW BOARD DOCUMENTS

PARTICIPANT CONSENT FORM

1. **Introduction.** You are invited to participate in a study of signature biometrics with a focus on keystroke dynamics. With signature information gathered from you and other participants, I hope to discover acceptable false acceptance and false rejection rates for signature-based biometrics. I ask you to read and sign this form indicating that you agree to be in the study. Please ask any questions you may have before signing.
2. **Background Information.** The Naval Postgraduate School COASTS field experimentation is conducting this study as part of an identity management research program entitled Biometric Identification Testing & Evaluation.
3. **Procedures.** If you agree to participate in this study, the researcher will explain the tasks in detail. There will be two sessions: a) 15 minute initial phase and 2) 30 minute follow-up phase, during which you will repeat your signature under various conditions related to signature-based biometrics.
4. **Risks and Benefits.** This research involves no risks or discomforts greater than those encountered at your local supermarket when signing the signature pad. The benefits to the participants are gaining a greater understanding of signature biometrics and the value of a unique, repeatable signature.
5. **Compensation.** No tangible reward will be given. A copy of the results will be available to you at the conclusion of the experiment.
6. **Confidentiality.** The records of this study will be kept confidential. No information will be publicly accessible which could identify you as a participant.
7. **Voluntary Nature of the Study.** If you agree to participate, you are free to withdraw from the study at any time without prejudice. You will be provided a copy of this form for your records.
8. **Points of Contact.** If you have any further questions or comments after the completion of the study, you may contact the research supervisor, James Ehler, at 831-656-3000, jfehlert@nps.edu.
9. **Statement of Consent.** I have read the above information. I have asked all questions and have had my questions answered. I agree to participate in this study.

Participant's Signature

Date

Researcher's Signature

Date

MINIMAL RISK CONSENT STATEMENT
NAVAL POSTGRADUATE SCHOOL, MONTEREY, CA 93943

Participant: VOLUNTARY CONSENT TO BE A RESEARCH PARTICIPANT IN: Testing & Evaluation of DynaSig Biometric Pen and Private Lock Infrastructure (PLI) in Support of Tactical Military and Law Enforcement Missions.

1. I have read, understand and been provided "Information for Participants" that provides the details of the below acknowledgments.
2. I understand that this project involves research. An explanation of the purposes of the research, a description of procedures to be used, identification of experimental procedures, and the extended duration of my participation have been provided to me.
3. I understand that this project does not involve more than minimal risk. I have been informed of any reasonably foreseeable risks or discomforts to me.
4. I have been informed of any benefits to me or to others that may reasonably be expected from the research.
5. I have signed a statement describing the extent to which confidentiality of records identifying me will be maintained.
6. I have been informed of any compensation and/or medical treatments available if injury occurs and is so, what they consist of, or where further information may be obtained.
7. I understand that my participation in this project is voluntary; refusal to participate will involve no penalty or loss of benefits to which I am otherwise entitled. I also understand that I may discontinue participation at any time without penalty or loss of benefits to which I am otherwise entitled.
8. I understand that the individual to contact should I need answers to pertinent questions about the research and about my rights as a research participant or concerning a research related injury is Mr. James Ehlert, Principal Investigator, Information Sciences Department. A full and responsive discussion of the elements of this project and my consent has taken place.
NPS Medical Advisor: LTC Eric Morgan, MC, USA, Commanding Officer, Presidio of Monterey Medical Clinic, (831) 242-7550, eric.morgan@nw.amedd.army.mil

Signature of Principal Investigator Date

Signature of Volunteer Date

PRIVACY ACT STATEMENT

NAVAL POSTGRADUATE SCHOOL, MONTEREY, CA 93943
PRIVACY ACT STATEMENT

1. Purpose: Signature biometric data will be collected to further understand the biometric advantage of a unique and evolving signature
2. Use: This data will be used for statistical analysis by the Departments of the Navy and Defense, and other U.S. Government agencies, provided this use is compatible with the purpose for which the information was collected. Use of the information may be granted to legitimate non-government agencies or individuals by the Naval Postgraduate School in accordance with the provisions of the Freedom of Information Act.
3. Disclosure/Confidentiality:
 - a. I have been assured that my privacy will be safeguarded. I will be assigned a control or code number which thereafter will be the only identifying entry on any of the research records. The Principal Investigator will maintain the cross-reference between name and control number. It will be decoded only when beneficial to me or if some circumstances, which is not apparent at this time, would make it clear that decoding would enhance the value of the research data. In all cases, the provisions of the Privacy Act Statement will be honored.
 - b. I understand that a record of the information contained in this Consent Statement or derived from the experiment described herein will be retained permanently at the Naval Postgraduate School or by higher authority. I voluntarily agree to its disclosure to agencies or individuals indicated in paragraph 3 and I have been informed that failure to agree to such disclosure may negate the purpose for which the experiment was conducted.
 - c. I also understand that disclosure of the requested information is voluntary.

Name, Grade/Rank (if applicable)
[Please print]

Signature of Volunteer

Date

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. Herbst, N.M., and Liu, C.N., "Automatic Signature Verification Based on Accelerometry," *IBM Journal of Research Development*, vol. 21, no. 3, pp. 245-253, May 1977.
2. Wessels, T., and Omlin, C.W., "A Hybrid System for Signature Verification," *Neural Networks*, pp. 509-514, 2000.
3. Fairhurst, M.C., "Signature Verification Revisited: Promoting Practical Exploitation of Biometric Technology," *Electronics and Communication Engineering Journal*, pp. 273-280, December 1997.
4. Ortega-Garcia, J., Bigun, J., Reynolds, D., and Gonzalez-Rodriguez, J., "Authentication Gets Personal with Biometric," *IEEE Signal Processing Magazine*, vol. 21, pp. 50-62, March 2004.
5. "Understanding Signature Verification," [<http://www.findbiometrics.com/Pages/signature%20articles/signatur...>], 25 February 2007.
6. Faundez-Zanuy, M., "Signature Recognition State-of-the-Art," *IEEE AandE Systems Magazine*, July 2005.
7. Tech Republic, "Reduce Multi-Factor Authentication Costs with Behavioral Biometrics," [<http://articles.techrepublic.com.com/5102-1009-6150761>]. 25 February 2007.
8. Gamassi, M., and others, "Accuracy and Performance of Biometric Systems," *Instrumentation and Measurement Technology Conference*, 2004, Proceedings of the 21st IEEE, vol. 1, pp. 510-515, May 2004.
9. Jain, A. K., Ross, A., and Pankanti, S., "Biometrics: A Tool for Information Security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125-143, June 2006.
10. Zimmerman, T., and others, "Retail Applications of Signature Verification," *Biometric Technology for Human Identification*, Proceedings of the SPIE, vol. 5404, pp. 206-214, August 2004.
11. DynaSig, Inc., *Bio-Pen® Solution Electronic Authentication, Access and Approval*, DynaSig, Inc., Phoenix, AZ, January 2006.
12. Yun, Y. W., "The '123' of Biometric Technology," [www.itsc.org.sg/synthesis/2002/biometric.pdf], 25 February 2007.

13. Liu, S., and Silverman, M., "A Practical Guide to Biometric Security Technology," *IEEE Computer Society, IT Pro-Security*, pp. 27-32, January-February 2001.
14. DynaSig, Inc., *DynaSig Bio-Pen® Banking Answers To:*, DynaSig, Inc., Phoenix, AZ.
15. Gaudreau, M., "The Distinction Between Biometric and Digital Signatures," [<http://www.findbiometrics.com/Pages/signature%20articles/signatur...>], 25 February 2007.
16. DynaSig, Inc., *Bio-Pen® Banking Solution*, DynaSig, Inc., Phoenix, AZ.
17. Email correspondence with Dr. Richard Kim, developer of the Bio-Pen and CEO of Dynamic Biometric Systems, Inc., November 2006 - March 2007.
18. DynaSig, Inc., *Bio-Pen® Web Client (R.2.1) and Lock Box (R.3.1) User Guide*, DynaSig, Inc., Phoenix, AZ, 2007.
19. DynaSig, Inc., *About DynaSig*, DynaSig, Inc., Phoenix, AZ.
20. DynaSig, Inc., *Bio-Pen® Lockbox (BPL) – Personal*, DynaSig, Inc., Phoenix, AZ, September 2006.
21. DynaSig, Inc., *Bio-Pen® Lockbox (BPL) – Professional*, DynaSig, Inc., Phoenix, AZ, September 2006.
22. DynaSig, Inc., *Bio-Pen® Lockbox (BPL) – Enterprise*, DynaSig, Inc., Phoenix, AZ, September 2006.
23. DynaSig, Inc., *The Most Versatile and Secure System for Data and Communications Protection*, DynaSig, Inc., Phoenix, AZ.
24. Kim, R., "Bio-Pen® White Paper Security Features," Dynasig Corporation, Tempe, AZ, 2005.
25. DynaSig, Inc., *Bio-Pen® Software, Driver and Hardware Installation Guide*, DynaSig, Inc., Phoenix, AZ, 2006.
26. Mansfield, A.J. and Wayman, J.L., *Best Practices in Testing and Reporting Performance of Biometric Devices Version 2.01*, National Physical Laboratory Report CMSC 14/02, August 2002.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Richard Kim
DynaSig Corporation
Phoenix, Arizona
4. Thomas Latta
C4ISR and IO PM
Space and Naval Warfare Systems Command
2721 C4ISR SEandIM Division, SSC-SD
80 Dept, 86 CND/IO OTandE Branch, COMOPTEVFOR
DOTandE IAandI/O OTandE Assessment Programs
San Diego, California
5. David Tinsley
Team Lead NPS GINA
Los Gatos, California
6. James F. Ehlert
Naval Postgraduate School
Monterey, California
7. Pat Sankar
Naval Postgraduate School
Monterey, California
8. Gurminder Singh
Naval Postgraduate School
Monterey, California
9. Edward Fisher
Naval Postgraduate School
Monterey, California
10. WendyWalsh
Naval Postgraduate School
Monterey, California

11. Nancy Ann Budden
Naval Postgraduate School
Monterey, California
12. Gerry Christman
OSD-NII
Washington, D.C.
13. Al Miller
2564 Veronica Lane
Woodbridge, Virginia
14. Peter Verga
Office of the Assistant Secretary for Homeland Defense
2600 Defense Pentagon
Room 5B 414
Washington, D.C.
15. Linton Wells II
Office of the Secretary of Defense
Pentagon
Washington, D.C.